UNIT 1 INTRODUCTION TO INFORMATION SECURITY

1.1 INFORMATION SECURITY

Introduction

Information security protects sensitive information from unauthorized activities, including inspection, modification, recording, and any disruption or destruction. The goal is to ensure the safety and privacy of critical data such as customer account details, financial data or intellectual property.

Security

In general, security is "the quality or state of being secure to be free from danger." In other words, protection against adversaries from those who would do harm, intentionally or otherwise is the objective. National security, for example, is a multilayered system that protects the sovereignty of a state, its assets, its resources, and its people. Achieving the appropriate level of security for an organization also requires a multifaceted system.

Multiple Layers of Security

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

1. **Physical Security :** Physical security, to protect physical items, objects, or areas from unauthorized access and misuse.
2. **Personnel Security :** Personnel security, to protect the individual or group of individuals who are authorized to access the organization and its operations.
3. **Operations Security :** Operations Security, to protect the details of a particular operation or series of activities.
4. **Communications Security :** Communications security, to protect communications media, technology, and content.
5. **Network Security :** Network security, to protect networking components, connections, and contents.

6. **Information Security :** Information security, to protect the confidentiality, integrity and availability of information assets, whether in storage, processing, or transmission. It is achieved via the application of policy, education, training and awareness, and technology.

CIA Triangle

The Committee on National Security Systems (CNSS) defines information security as the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information.12 Figure 1-3 shows that information security includes the broad areas of information security management, computer and data security, and network security. The CNSS model of information security evolved from a concept developed by the computer security industry called the C.I.A. triangle.

The C.I.A. triangle has been the industry standard for computer security since the development of the mainframe. It is based on the three characteristics of information that give it value to organizations: confidentiality, integrity, and availability.

The C.I.A. triangle - confidentiality, integrity, and availability - has expanded into a more comprehensive list of critical characteristics of information. At the heart of the study of information security is the concept of policy. Policy, awareness, training, education, and technology are vital concepts for the protection of information and for keeping information systems from danger.

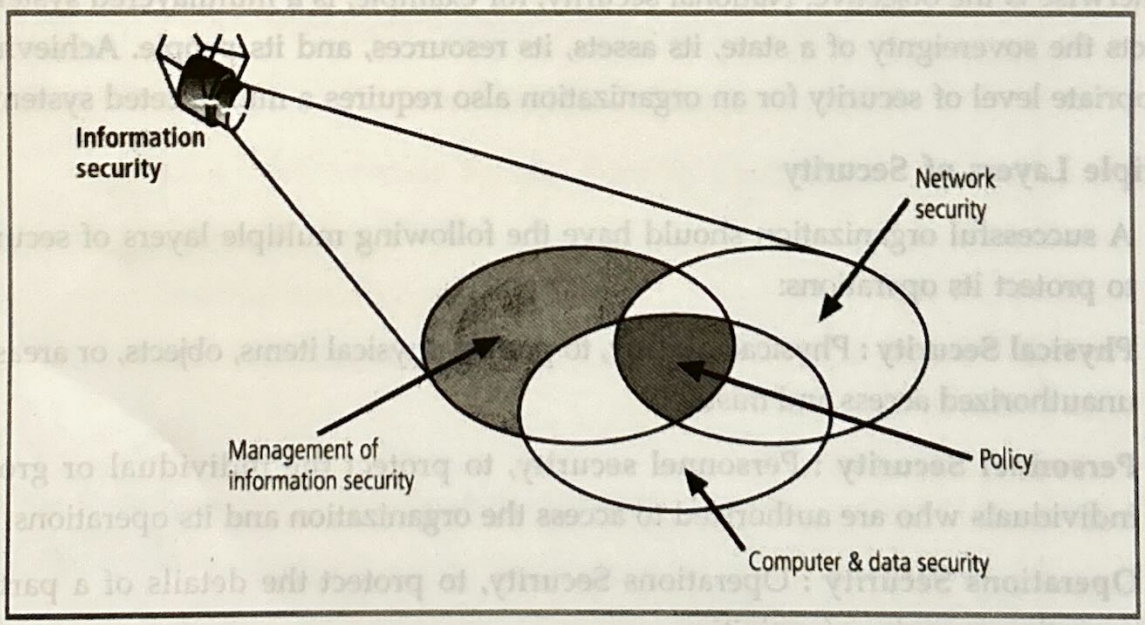

Fig : Components of Information Security

The three components of the CIA triad are discussed below:

1. **Confidentiality:** This component is often associated with secrecy and the use of encryption. Confidentiality in this context means that the data is only available to

authorized parties. When information has been kept confidential it means that it has not been compromised by other parties; confidential data are not disclosed to people who do not require them or who should not have access to them. Ensuring confidentiality means that information is organized in terms of who needs to have access, as well as the sensitivity of the data. A breach of confidentiality may take place through different means, for instance hacking or social engineering.

2. **Integrity:** Data integrity refers to the certainty that the data is not tampered with or degraded during or after submission. It is the certainty that the data has not been subject to unauthorized modification, either intentional or unintentional. There are two points during the transmission process during which the integrity could be compromised: during the upload or transmission of data or during the storage of the document in the database or collection.

3. **Availability:** This means that the information is available to authorized users when it is needed. For a system to demonstrate availability, it must have properly functioning computing systems, security controls and communication channels. Systems defined as critical (power generation, medical equipment, safety systems) often have extreme requirements related to availability. These systems must be resilient against cyber threats, and have safeguards against power outages, hardware failures and other events that might impact the system availability.

1.1.1 History of Information Security

These days, information plays an important role in day to day lives of every individual, whether it be a high profile businessman to being a small shop owner. Information is generated in different forms from being their Smartphone's to their transaction receipts and buying patterns. This presents a wealth of opportunities for people to steal data; that is why information security is a necessity.

1960s: Offline sites security: The Information Security was limited to the access points where computers were stored, as they used to be large in sizes and required a huge area to be stored and operated. Multiple layers of security were installed over terminals in form of passwords and other security measures.

1970s: Evolution of personal computer and hackers: At this time there was no massive global network connecting every device that wanted to be connected. Only large organizations, especially governments, were starting to link computers via telephone lines and peoples started to seek different ways to intercept the information flowing through those telephone lines in order to steal the data and these group of peoples became the first hackers.

1980s: Evolution of cyber-crime: Hacking and other forms of cyber crimes skyrocketed in this decade with people finding different ways to break into the computer systems and being no strict regulation against the hackers it was a booming craze for the youth. Many government & Military groups were on the receiving end of these crimes with loss of over millions of dollars from U.S. Banks and in response to this the government started pursuing the hackers.

1990s: "Hacking" becoming an organized crime: After the worldwide web was made available in 1989, people started putting their personal information online; hackers saw this as a potential revenue source, and started to steal data from people and governments via the web. Firewalls and antivirus programs helped protect against this, but the web was a mostly unsecured with hackers finding different ways to infiltrate the targets devices.

2000s: Cybercrime becoming a serious issue: Hacking wasn't considered as serious issues in late 80's but with evolution of hacking and their dangers governments started chasing the cyber criminals. Strong measures were taken against cyber criminals, hackers were jailed for years as punishment for cyber criminal activity and cyber security cells were formed in order to deal with the issues involving any form of cyber crime.

2010s: Information security as we know it: Although different measures in form of firewalls and antivirus were designed to protect the devices from attacks but hackers who were efficient and skilled enough were able to breach the systems anyway. Different cryptographic algorithms and encryption techniques are being used in order to protect the data over network and other transmission mediums. Different organizations also implement security policies to avoid human errors of breaching the data in different ways. Software and antivirus programs are installed on PC's to protect them from the outside attacks. With time as the internet and devices surrounding the internet evolved, the threat to the information security also found many ways to breach into them. Information security plays a major role in day to day life of every person and organizations.

1.1.2 Critical Characteristics of Information

The critical characteristic of information that is the expanded C.I.A. triangle is defined in the sections below.

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.

2. **Accuracy** : Information has accuracy when it is free from mistakes or errors and it has the value that the end user expects. If information has been intentionally or unintentionally modified, it is no longer accurate. Consider, for example, a checking account. You assume that the information contained in your checking account is an accurate representation of your finances. Incorrect information in your checking account can result from external or internal errors. If a bank teller, for instance, mistakenly adds or subtracts too much from your account, the value of the information is changed. Or, you may accidentally enter an incorrect amount into your account register. Either way, an inaccurate bank balance could cause you to make mistakes, such as bouncing a check.

3. **Authenticity** : Authenticity of information is the quality or state of being genuine or original, rather than a reproduction or fabrication. Information is authentic when it is in the same state in which it was created, placed, stored, or transferred. Consider for a moment some common assumptions about e-mail. When you receive e-mail, you assume that a specific individual or group created and transmitted the e-mail—you assume you know the origin of the e-mail. This is not always the case.

   E-mail spoofing, the act of sending an e-mail message with a modified field, is a problem for many people today, because often the modified field is the address of the originator. Spoofing the sender's address can fool e-mail recipients into thinking that messages are legitimate traffic, thus inducing them to open e-mail they otherwise might not have. Spoofing can also alter data being transmitted across a network, as in the case of user data protocol (UDP) packet spoofing, which can enable the attacker to get access to data stored on computing systems.

4. **Confidentiality :** Information has confidentiality when it is protected from disclosure or exposure to unauthorized individuals or systems. Confidentiality ensures that only those with the rights and privileges to access information are able to do so. When unauthorized individuals or systems can view information, confidentiality is breached.

5. **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.

7. **Utility :** The utility of information is the quality or state of having value for some purpose or end. Information has value when it can serve a purpose. If information is

available, but is not in a format meaningful to the end user, it is not useful. For example, to a private citizen U.S. Census data can quickly become overwhelming and difficult to interpret; however, for a politician, U.S. Census data reveals information about the residents in a district, such as their race, gender, and age. This information can help form a politician's next campaign strategy.

8. **Possession :** The possession of information is the quality or state of ownership or control. Information is said to be in one's possession if one obtains it, independent of format or other characteristics. While a breach of confidentiality always results in a breach of possession, a breach of possession does not always result in a breach of confidentiality.

1.1.3 NSTISSC Security Model

CNSS Security Model

The definition of information security presented in this text is based in part on the CNSS document called the National Training Standard for Information Systems Security Professionals NSTISSI. 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.

The library of documents is being renamed as the documents are rewritten. This document presents a comprehensive information security model and has become a widely accepted evaluation standard for the security of information systems. The model, created by John McCumber in 1991, provides a graphical representation of the architectural approach widely used in computer and information security; it is now known as the **McCumber Cube** The McCumber Cube in Figure shows three dimensions.

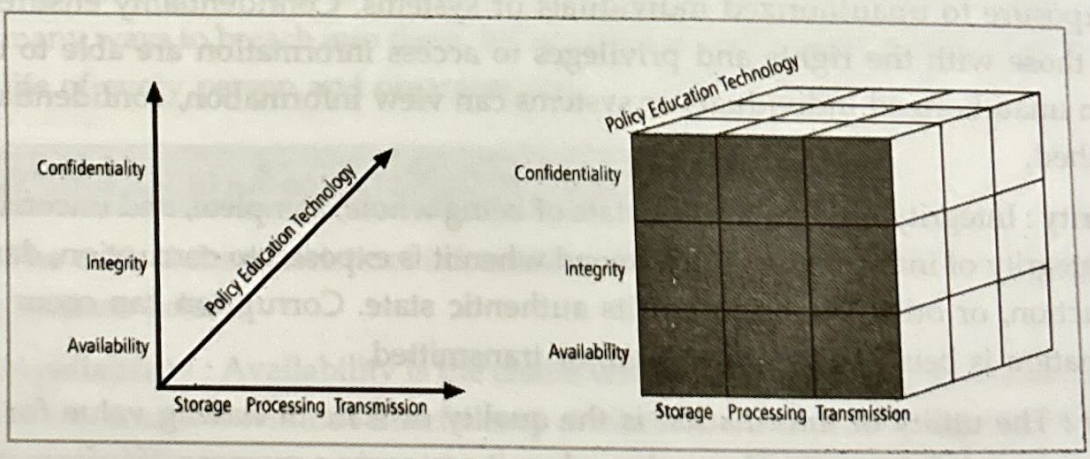

Fig : The McCumber Cube

The 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 & storage areas 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.

1.1.4 Components of an Information System - Securing the Components

The six critical components enable information to be input, processed, output, and stored. Each of these IS components has its own strengths and weaknesses, as well as its own characteristics and uses. Each component of the information system also has its own security requirements.

As shown in Figure, an information system (IS) is much more than computer hardware; it is the entire set of software, hardware, data, people, procedures, and networks that make possible the use of information resources in the organization.

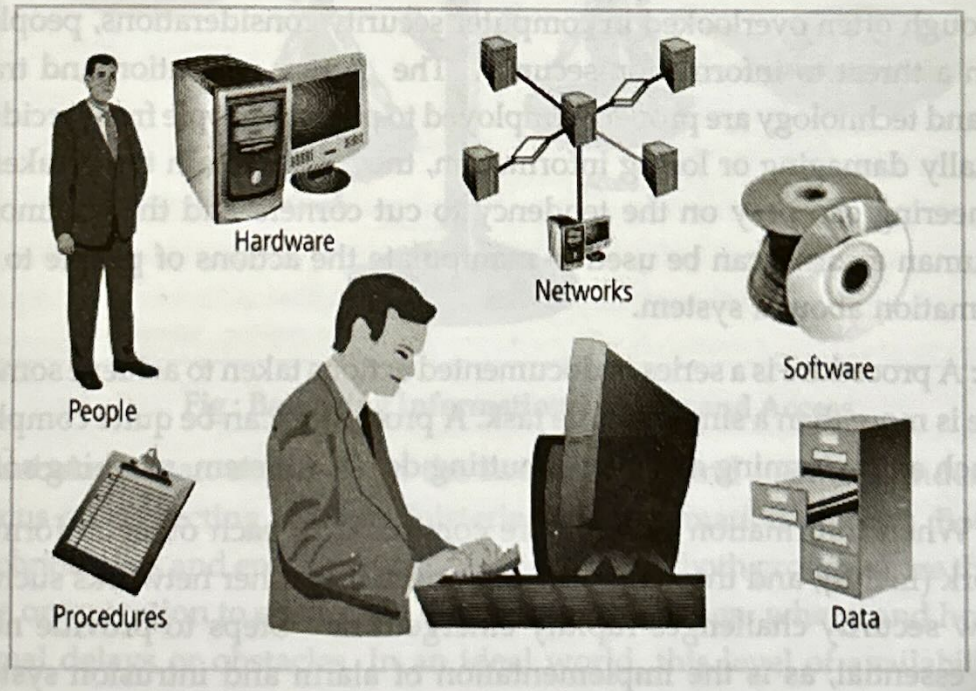

Fig.: Components of an Information System

1. **Software :** The software components of IS comprises applications, operating systems, and assorted command utilities. 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.

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

3. **Data :** Data stored, processed, and transmitted by a computer system must be protected. Data is often the most valuable asset possessed by an organization and it is the main target of intentional attacks. Systems developed in recent years are likely to make use of database management systems. When done properly, this should improve the security of the data and the application. Unfortunately, many system development projects do not make full use of the database management system's security capabilities, and in some cases the database is implemented in ways that are less secure than traditional file systems.

4. **People** : Though often overlooked in computer security considerations, people have always been a threat to information security. The 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. Social engineering can prey on the tendency to cut corners and the commonplace nature of human error. It can be used to manipulate the actions of people to obtain access information about a system.

5. **Procedures :** 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.

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. The Steps to provide network security are essential, as is the implementation of alarm and intrusion systems to make system owners aware of ongoing compromises.

1.2 BALANCING SECURITY AND ACCESS

Even with the best planning and implementation, it is impossible to obtain perfect information security. Recall James Anderson's statement from the beginning of this concept, 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.

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.

Figure shows some of the competing voices that must be considered when balancing information security and access. Because of today's security concerns and issues, an information system or data-processing department can get too entrenched in the management and protection of systems.

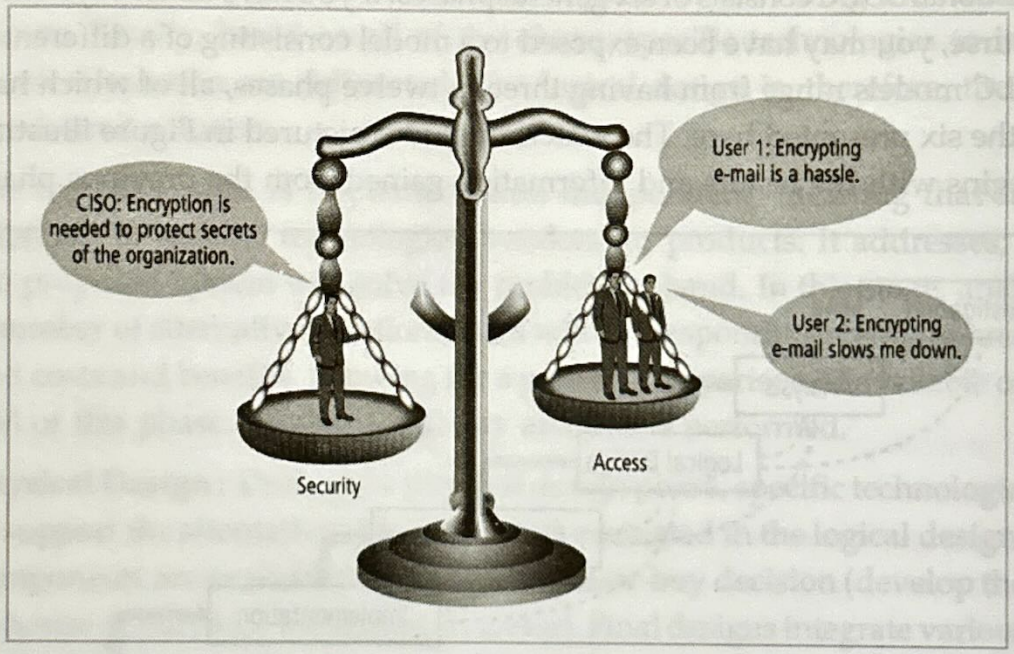

Fig : Balancing Information Security and Access

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.

1.3 THE SYSTEMS DEVELOPMENT LIFE CYCLE (SDLC)

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 place is to use a variation of the systems development life cycle (SDLC): the security systems development life cycle (SecSDLC). To understand a security systems development life cycle, you must first understand the basics of the method upon which it is based.

Methodology and Phases of SDLC)

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. Once a methodology has been adopted, the key milestones are established and a team of individuals is selected and made accountable for accomplishing the project goals.

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.

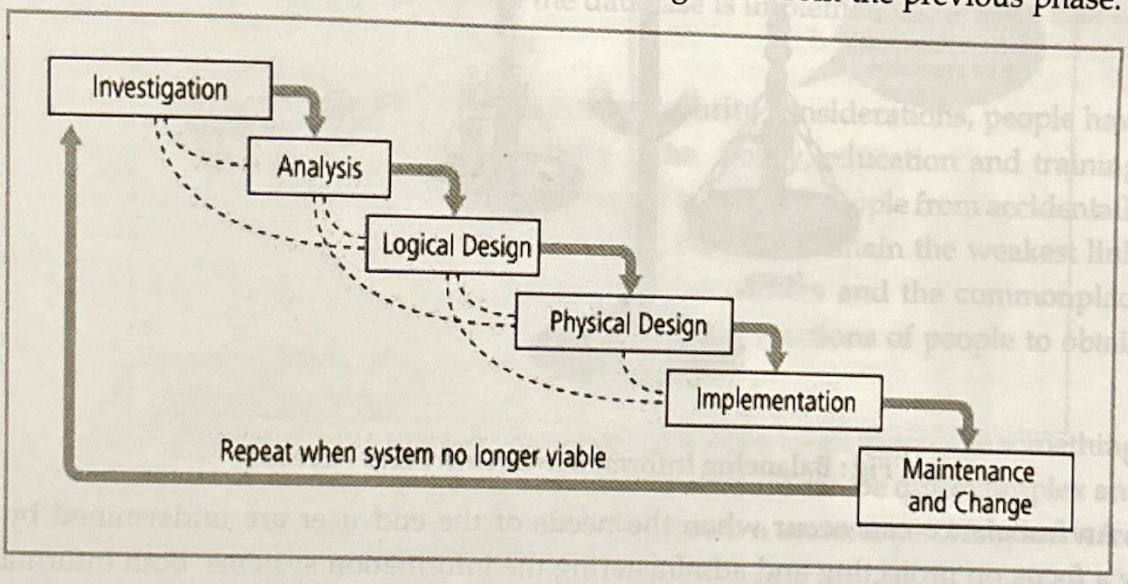

Fig : SDLC Waterfall Methodology

The following sections describe each phase of the traditional SDLC.

1. **Investigation :** The first phase, investigation, is the most important. The investigation phase begins with an examination of the event or plan that initiates the process.

During the investigation phase, the objectives, constraints, and scope of the project are specified. A preliminary cost-benefit analysis evaluates the perceived benefits and the appropriate levels of cost for those benefits. At the conclusion of this phase, and at every phase following, a feasibility analysis assesses the economic, technical, and behavioral feasibilities of the process and ensures that implementation is worth the organization's time and effort.

2. **Analysis :** The analysis phase begins with the information gained during the investigation phase. This phase consists primarily of assessments of the organization, its current systems, and its 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.

3. **Logical Design** : In the logical design phase, the information gained from the analysis phase is used to begin creating a systems solution for a business problem. In any systems solution, it is imperative that the first and driving factor is the business need. Based on the business need, applications are selected to provide needed services, and then data support and structures capable of providing the needed inputs are chosen. Finally, based on all of the above, specific technologies to implement the physical solution are delineated. The logical design is, therefore, the blueprint for the desired solution.

   The logical design is implementation independent, meaning that it contains no reference to specific technologies, vendors, or products. It addresses, instead, how the proposed system will solve the problem at hand. In this stage, analysts generate a number of alternative solutions, each with corresponding strengths and weaknesses, and costs and benefits, allowing for a general comparison of available options. At the end of this phase, another feasibility analysis is performed.

4. **Physical Design :** During the physical design phase, specific technologies are selected to support the alternatives identified and evaluated in the logical design. The selected components are evaluated based on a make-or-buy decision (develop the components in-house or purchase them from a vendor). Final designs integrate various components and technologies. After yet another feasibility analysis, the entire solution is presented to the organizational management for approval.

5. **Implementation** : In the implementation phase, any needed software is created. Components are ordered, received, and tested. Afterward, users are trained and supporting documentation created. Once all 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.

6. **Maintenance and Change :** The maintenance and change phase is the longest and most expensive phase of the process. This phase consists of the tasks necessary to support and modify the system for the remainder of its useful life cycle. Even though formal development may conclude during this phase, the life cycle of the project continues until it is determined that the process should begin again from the investigation phase. At periodic points, the system is tested for compliance, and the feasibility of continuance versus discontinuance is evaluated. Upgrades, updates, and patches are managed.

As the needs of the organization change, the systems that support the organization must also change. It is imperative that those who manage the systems, as well as those who support them, continually monitor the effectiveness of the systems in relation to the organization's environment. When a current system can no longer support the evolving mission of the organization, the project is terminated and a new project is implemented.

1.4 THE SECURITY 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. This means that each implementation of a system is secure and does not risk compromising the confidentiality, integrity, and availability of the organization's information assets. The following section, adapted from NIST Special Publication 800-64, rev. 1, provides an overview of the security considerations for each phase of the SDLC.

Each of the example SDLC phases [discussed earlier] includes a minimum set of security steps needed to effectively incorporate security into a system during its development. An organization will either use the general SDLC described [earlier] or will have developed a tailored SDLC that meets their specific needs. In either case, NIST recommends that organizations incorporate the associated IT security steps of this general SDLC into their development process:

1. **Investigation/Analysis Phases**

   A. **Security categorization :** defines three levels (i.e., low, moderate, or high) of potential impact on organizations or individuals should there be a breach of security (a loss of confidentiality, integrity, or availability). Security categorization standards assist organizations in making the appropriate selection of security controls for their information systems.

B. **Preliminary risk assessment:** Results in an initial description of the basic security needs of the system. A preliminary risk assessment should define the threat environment in which the system will operate.

2. **Logical/Physical Design Phases**

A. **Risk assessment:** Analysis that identifies the protection requirements for the system through a formal risk assessment process. This analysis builds on the initial risk assessment performed during the Initiation phase, but will be more in-depth and specific.

B. **Security functional requirements analysis :** Analysis of requirements that may include the following components: (1) system security environment (i.e., enterprise information security policy and enterprise security architecture) and (2) security functional requirements

C. **Security assurance requirements analysis** :Analysis of requirements that address the developmental activities required and assurance evidence needed to produce the desired level of confidence that the information security will work correctly and effectively. The analysis, based on legal and functional security requirements, will be used as the basis for determining how much and what kinds of assurance are required.

D. **Cost considerations and reporting :** Determines how much of the development cost can be attributed to information security over the life cycle of the system. These costs include hardware, software, personnel, and training.

E. **Security planning :** Ensures that agreed upon security controls, planned or in place, are fully documented. The security plan also provides a complete characterization or description of the information system as well as attachments or references to key documents supporting the agency's information security program (e.g., configuration management plan, contingency plan, incident response plan, security awareness and training plan, rules of behavior, risk assessment, security test and evaluation results, system interconnection agreements, security authorizations/ accreditations, and plan of action and milestones).

F. **Security control development :** Ensures that security controls described in the respective security plans are designed, developed, and implemented. For information systems currently in operation, the security plans for those systems may call for the development of additional security controls to supplement the controls already in place or the modification of selected controls that are deemed to be less than effective.

G. **Developmental security test and evaluation:** Ensures that security controls developed for a new information system are working properly and are effective. Some types of security controls (primarily those controls of a non-technical nature) cannot be tested

and evaluated until the information system is deployed—these controls are typically management and operational controls.

H. **Other planning components**—ensures that all necessary components of the development process are considered when incorporating security into the life cycle. These components include selection of the appropriate contract type, participation by all necessary functional groups within an organization, participation by the certifier and accreditor, and development and execution of necessary contracting plans and processes.

3. **Implementation Phase**

A. **Inspection and acceptance** :ensures that the organization validates and verifies that the functionality described in the specification is included in the deliverables.

System integration—ensures that the system is integrated at the operational site where the information system is to be deployed for operation. Security control settings and switches are enabled in accordance with vendor instructions and available security implementation guidance.

B. **Security certification :** ensures that the controls are effectively implemented through established verification techniques and procedures and gives organization officials confidence that the appropriate safeguards and countermeasures are in place to protect the organization's information system. Security certification also uncovers and describes the known vulnerabilities in the information system.

C. **Security accreditation:** provides the necessary security authorization of an information system to process, store, or transmit information that is required. This authorization is granted by a senior organization official and is based on the verified effectiveness of security controls to some agreed upon level of assurance and an identified residual risk to agency assets or operations.

4. **Maintenance and Change Phase**

A. **Configuration management and control:** ensures adequate consideration of the potential security impacts due to specific changes to an information system or its surrounding environment. Configuration management and configuration control procedures are critical to establishing an initial baseline of hardware, software, and firmware components for the information system and subsequently controlling and maintaining an accurate inventory of any changes to the system.

B. **Continuous monitoring:**ensures that controls continue to be effective in their application through periodic testing and evaluation. Security control monitoring (i.e., verifying the continued effectiveness of those controls over time) and reporting the

security status of the information system to appropriate agency officials is an essential activity of a comprehensive information security program.

C. **Information preservation** : ensures that information is retained, as necessary, to conform to current legal requirements and to accommodate future technology changes that may render the retrieval method obsolete.

D. **Media sanitization** : ensures that data is deleted, erased, and written over as necessary.

E. **Hardware and software disposal**:ensures that hardware and software is disposed of as directed by the information system security officer.

Adapted from Security Considerations in the Information System Development Life Cycle.

It is imperative that information security be designed into a system from its inception, rather than added in during or after the implementation phase. Information systems that were designed with no security functionality, or with security functions added as an afterthought, often require constant patching, updating, and maintenance to prevent risk to the systems and information. It is a well-known adage that "an ounce of prevention is worth a pound of cure." With this in mind, organizations are moving toward more security-focused development approaches, seeking to improve not only the functionality of the systems they have in place, but consumer confidence in their products.

In early 2002, Microsoft effectively suspended development work on many of its products while it put its OS developers, testers, and program managers through an intensive program focusing on secure software development. It also delayed release of its flagship server operating system to address critical security issues. Many other organizations are following Microsoft's recent lead in putting security into the development process

1.5 NEED FOR SECURITY

The information technology program is the primary mission of an information security program is to ensure that systems and their contents remain the same. Organizations expend hundreds of thousands of dollars and thousands of man-hours to maintain their information systems. If threats to information and systems didn't exist, these resources could be used to improve the systems that support the information. However, attacks on information systems are a daily occurrence, and the need for information security grows along with the sophistication of such attacks.

Organizations must understand the environment in which information systems operate so that their information security programs can address actual and potential problems. This chapter describes this environment and identifies the threats it poses to organizations and their information.

1.5.1 Business Needs

The First Information security performs four important functions for an organization:

1. Protecting the organization's ability to function.
2. Enabling the safe operation of applications running on the organization's IT systems.
3. Protecting the data the organization collects and uses.
4. Safeguarding the organization's technology assets.

1. **Protecting the Functionality of an Organization :** Both general management and IT management are responsible for implementing information security that protects the organization's ability to function. Although many business and government managers shy away from addressing information security because they perceive it to be a technically complex task, in fact, implementing information security has more to do with management than with technology. Just as managing payroll has more to do with management than with mathematical wage computations, managing information security has more to do with policy and its enforcement than with the technology of its implementation.

2. **Enabling the Safe Operation of Applications** : Today's organizations are under immense pressure to acquire and operate integrated, efficient, and capable applications. A modern organization needs to create an environment that safeguards these applications, particularly those that are important elements of the organization's infrastructure—operating system platforms, electronic mail (e-mail), and instant messaging (IM) applications. Organizations acquire these elements from a service provider or they build their own. Once an organization's infrastructure is in place, management must continue to oversee it, and not relegate its management to the IT department.

3. **Protecting Data that Organizations Collect and Use :** Without data, an organization loses its record of transactions and/or its ability to deliver value to its customers. Any business, educational institution, or government agency operating within the modern context of connected and responsive services relies on information systems. Even when transactions are not online, information systems and the data they process enable the creation and movement of goods and services. Therefore, protecting data in motion and data at rest are both critical aspects of information security. The value of data motivates attackers to steal, sabotage, or corrupt it. An effective information security program implemented by management protects the integrity and value of the organization's data.

4. **Safeguarding Technology Assets in Organizations** : To perform effectively, organizations must employ secure infrastructure services appropriate to the size and scope of the enterprise. For instance, a small business may get by using an e-mail service provided by an ISP and augmented with a personal encryption tool. When an organization grows, it must develop additional security services. For example, organizational growth could lead to the need for public key infrastructure (PKI), an integrated system of software, encryption methodologies, and legal agreements that can be used to support the entire information infrastructure.

1.5.2 Threats

The categorization scheme consists of fourteen general categories that represent clear and present dangers to an organization's people, information, and systems. Each organization must prioritize the threats it faces, based on the particular security situation in which it operates, its organizational strategy regarding risk, and the exposure levels at which its assets operate.

1. Compromises to Intellectual Property

Many organizations create, or support the development of, intellectual property (IP) as part of their business operations .Intellectual property is defined as "the ownership of ideas and control over the tangible or virtual representation of those ideas. Use of another person's intellectual property may or may not involve royalty payments or permission, but should always include proper credit to the source."

Intellectual property can be trade secrets, copyrights, trademarks, and patents. The unauthorized appropriation of IP constitutes a threat to information security. Employees may have access privileges to the various types of IP, and may be required to use the IP to conduct day-to-day business.

Organizations often purchase or lease the IP of other organizations, and must abide by the purchase or licensing agreement for its fair and responsible use. The most common IP breach is the unlawful use or duplication of software-based intellectual property, more commonly known as software piracy. Many individuals and organizations do not purchase software as mandated by the owner's license agreements. Because most software is licensed to a particular purchaser, its use is restricted to a single user or to a designated user in an organization.

If the user copies the program to another computer without securing another license or transferring the license, he or she has violated the copyright.

2. Deliberate Software Attacks

Deliberate software attacks occur when an individual or group designs and deploys software to attack a system. Most of this software is referred to as **malicious code** or

malicious software, or sometimes **malware**. These software components or programs are designed to damage, destroy, or deny service to the target systems. Some of the more common instances of malicious code are viruses and worms, Trojan horses, logic bombs, and back doors.

3. Deviations in Quality of Service

An organization's information system depends on the successful operation of many interdependent support systems, including power grids, telecom networks, parts suppliers, service vendors, and even the janitorial staff and garbage haulers. Any one of these support systems can be interrupted by storms, employee illnesses, or other unforeseen events.

Deviations in quality of service can result from incidents such as a backhoe taking out a fiber-optic link for an ISP. The backup provider may be online and in service, but may be able to supply only a fraction of the bandwidth the organization needs for full service.

This degradation of service is a form of **availability disruption**. Irregularities in Internet service, communications, and power supplies can dramatically affect the availability of information and systems.

A. **Internet Service Issues :** In organizations that rely heavily on the Internet and the World Wide Web to support continued operations, Internet service provider failures can considerably undermine the availability of information. Many organizations have sales staff and telecommuters working at remote locations. When these offsite employees cannot contact the host systems, they must use manual procedures to continue operations.

B. **Communications and Other Service Provider Issues :** Other utility services can affect organizations as well. Among these are telephone, water, wastewater, trash pickup, cable television, natural or propane gas, and custodial services. The loss of these services can impair the ability of an organization to function. For instance, most facilities require water service to operate an air-conditioning system. Even in Minnesota in February, airconditioning systems help keep a modern facility operating. If a wastewater system fails, an organization might be prevented from allowing employees into the building.

C. **Power Irregularities :** Irregularities from power utilities are common and can lead to fluctuations such as power excesses, power shortages, and power losses. This can pose problems for organizations that provide inadequately conditioned power for their information systems equipment.

4. Espionage or Trespass

Espionage or trespass is a well-known and broad category of electronic and human activities that can breach the confidentiality of information. When an unauthorized individual gains access to the information an organization is trying to protect, that act is categorized as espionage or trespass. Attackers can use many different methods to access the information stored in an information system. Some information gathering techniques are quite legal, for example, using a Web browser to perform market research. These legal techniques are called, collectively, competitive intelligence. When information gatherers employ techniques that cross the threshold of what is legal or ethical, they are conducting industrial espionage.

Many countries considered allies of the United States engage in industrial espionage against American organizations. When foreign governments are involved, these activities are considered espionage and a threat to national security. Some forms of espionage are relatively low tech.

5. Forces of Nature

Forces of nature, force majeure, or acts of God can present some of the most dangerous threats, because they usually occur with very little warning and are beyond the control of people. These threats, which include events such as fires, floods, earthquakes, and lightning as well as volcanic eruptions and insect infestations, can disrupt not only the lives of individuals but also the storage, transmission, and use of information.

Some of the more common threats in this group are listed here.

a. **Fire**: In this context, usually a structural fire that damages a building housing computing equipment that comprises all or part of an information system, as well as smoke damage and/or water damage from sprinkler systems or firefighters. This threat can usually be mitigated with fire casualty insurance and/or business interruption insurance.

b. **Flood**: An overflowing of water onto an area that is normally dry, causing direct damage to all or part of the information system or to the building that houses all or part of the information system. A flood might also disrupt operations through interruptions in houses it, and can also disrupt operations through interruptions in access to the buildings that house all or part of the information system. This threat can sometimes be mitigated with specific casualty insurance and/or business interruption insurance, but is usually a separate policy.

c. **Lightning**: An abrupt, discontinuous natural electric discharge in the atmosphere. Lightning usually directly damages all or part of the information system an/or its

power distribution components. It can also cause fires or other damage to the building that houses all or part of the information system, and disrupt operations by interfering with access to the buildings that house all or part of the information system. This threat can usually be mitigated with multipurpose casualty insurance and/or business interruption insurance.

d. **Landslide or Mudslide**: The downward sliding of a mass of earth and rock directly damaging all or part of the information system or, more likely, the building that houses it. Land or mudslides also disrupt operations by interfering with access to the buildings that house all or part of the information system. This threat can sometimes be mitigated with casualty insurance and/or business interruption insurance.

e. **Tornado or Severe Windstorm**: A rotating column of air ranging in width from a few yards to more than a mile and whirling at destructively high speeds, usually accompanied by a funnel-shaped downward extension of a cumulonimbus cloud. Storms can directly damage all or part of the information system or, more likely, the building that houses it, and can also interrupt access to the buildings that house all or part of the information system. This threat can sometimes be mitigated with casualty insurance and/or business interruption insurance.

f. **Hurricane or Typhoon**: A severe tropical cyclone originating in the equatorial regions of the Atlantic Ocean or Caribbean Sea or eastern regions of the Pacific Ocean (typhoon), travelling north, northwest, or northeast from its point of origin, and usually involving heavy rains. These storms can directly damage all or part of the information system or, more likely, the building that houses it. Organizations located in coastal or low-lying areas may experience flooding (see above). These storms may also disrupt operations by interrupting access to the buildings that house all or part of the information system. This threat can sometimes be mitigated with casualty insurance and/or business interruption insurance.

g. **Tsunami**: A very large ocean wave caused by an underwater earthquake or volcanic eruption. These events can directly damage all or part of the information system or, more likely, the building that houses it. Organizations located in coastal areas may experience tsunamis. Tsunamis may also cause disruption to operations through interruptions in access or electrical power to the buildings that house all or part of the information system. This threat can sometimes be mitigated with casualty insurance and/or business interruption insurance.

h. **Electrostatic Discharge (ESD)**: Usually, static electricity and ESD are little more than a nuisance. Unfortunately, however, the mild static shock we receive when walking

across a carpet can be costly or dangerous when it ignites flammable mixtures and damages costly electronic components. Static electricity can draw dust into clean-room environments or cause products to stick together. The cost of ESD-damaged electronic devices and interruptions to service can range from only a few cents to several millions of dollars for critical systems. Loss of production time in information processing due to ESD impact is significant. While not usually viewed as a threat, ESD can disrupt information systems, but it is not usually an insurable loss unless covered by business interruption insurance.

i. **Dust Contamination**: Some environments are not friendly to the hardware components of information systems. Because dust contamination can shorten the life of information systems or cause unplanned downtime, this threat can disrupt normal operations.

Since it is not possible to avoid force of nature threats, organizations must implement controls to limit damage, and they must also prepare contingency plans for continued operations, such as disaster recovery plans, business continuity plans, and incident response plans.

6. Human Error or Failure

This category includes acts performed without intent or malicious purpose by an authorized user. When people use information systems, mistakes happen. Inexperience, improper training, and the incorrect assumptions are just a few things that can cause these misadventures. Regardless of the cause, even innocuous mistakes can produce extensive damage.

One of the greatest threats to an organization's information security is the organization's own employees. Employees are the threat agents closest to the organizational data. Because employees use data in everyday activities to conduct the organization's business, their mistakes represent a serious threat to the confidentiality, integrity, and availability of data—data—even, suggests, relative to threats from outsiders.

7. Information Extortion

Information extortion occurs when an attacker or trusted insider steals information from a computer system and demands compensation for its return or for an agreement not to disclose it. Extortion is common in credit card number theft. For example, Web-based retailer CD Universe was the victim of a theft of data files containing customer credit card information.

The culprit was a Russian hacker named Maxus, who hacked the online vendor and stole several hundred thousand credit card numbers. When the company refused to pay

the $100,000 blackmail, he posted the card numbers to a Web site, offering them to the criminal community. His Web site became so popular he had to restrict access.

8. Missing, Inadequate, or Incomplete Organizational

Policy or Planning : Missing, inadequate, or incomplete organizational policy or planning makes an organization vulnerable to loss, damage, or disclosure of information assets when other threats lead to attacks. Information security is, at its core, a management function. The organization's executive leadership is responsible for strategic planning for security as well as for IT and business functions—a task known as governance.

9. Missing, Inadequate, or Incomplete Controls

Missing, inadequate, or incomplete controls—that is, security safeguards and information asset protection controls that are missing, misconfigured, antiquated, or poorly designed or managed—make an organization more likely to suffer losses when other threats lead to attacks. For example, if a small organization installs its first network using small office/ home office (SOHO) equipment (which is similar to the equipment you might have on your home network) and fails to upgrade its network equipment as it becomes larger, the increased traffic can affect performance and cause information loss. Routine security audits to assess the current levels of protection help to ensure the continuous protection of organization's assets.

10. Sabotage or Vandalism

This category of threat involves the deliberate sabotage of a computer system or business, or acts of vandalism to either destroy an asset or damage the image of an organization. These acts can range from petty vandalism by employees to organized sabotage against an Organization. Although not necessarily financially devastating, attacks on the image of an organization are serious. Vandalism to a Web site can erode consumer confidence, thus diminishing an organization's sales and net worth, as well as its reputation.

11. Theft

The threat of **theft**—the illegal taking of another's property, which can be physical, electronic, or intellectual—is a constant. The value of information is diminished when it is copied without the owner's knowledge. Physical theft can be controlled quite easily by means of a wide variety of measures, from locked doors to trained security personnel and the installation of alarm systems. Electronic theft, however, is a more complex problem to manage and control. When someone steals a physical object, the loss is easily detected; if it has any importance at all, its absence is noted. When electronic information is stolen, the

crime is not always readily apparent. If thieves are clever and cover their tracks carefully, no one may ever know of the crime until it is far too late.

12. Technical Hardware Failures or Errors

Technical hardware failures or errors occur when a manufacturer distributes equipment containing a known or unknown flaw. These defects can cause the system to perform outside of expected parameters, resulting in unreliable service or lack of availability. Some errors are terminal—that is, they result in the unrecoverable loss of the equipment. Some errors are intermittent, in that they only periodically manifest themselves, resulting in faults that are not easily repeated, and thus, equipment can sometimes stop working, or work in unexpected ways.

13. Technical Software Failures or Errors

Large quantities of computer code are written, debugged, published, and sold before all their bugs are detected and resolved. Sometimes, combinations of certain software and hardware reveal new bugs. These failures range from bugs to untested failure conditions. Sometimes these bugs are not errors, but rather purposeful shortcuts left by programmers for benign or malign reasons. Collectively, shortcut access routes into programs that bypass security checks are called trap doors and can cause serious security breaches.

Software bugs are so commonplace that entire Web sites are dedicated to documenting them. Among the most often used is Bugtraq, found at www.securityfocus.com, which provides up-to-the-minute information on the latest security vulnerabilities, as well as a very thorough archive of past bugs.

14. Technological Obsolescence

Antiquated or outdated infrastructure can lead to unreliable and untrustworthy systems. Management must recognize that when technology becomes outdated, there is a risk of loss of data integrity from attacks. Management's strategic planning should always include an analysis of the technology currently in use. Ideally, proper planning by management should prevent technology from becoming obsolete, but when obsolescence is manifest, management must take immediate action. IT professionals play a large role in the identification of probable obsolescence.

Recently, the software vendor Symantec retired support for a legacy version of its popular antivirus software, and organizations interested in continued product support were obliged to upgrade immediately to a different antivirus control software. In organizations where IT personnel had kept management informed of the coming retirement, these replacements were made more promptly and at lower cost than at organizations where the software was allowed to become obsolete.

1.5.3 Attacks

An attack is an act that takes advantage of a vulnerability to compromise a controlled system. It is accomplished by a threat agent that damages or steals an organization's information or physical asset. A vulnerability is an identified weakness in a controlled system, where controls are not present or are no longer effective. Unlike threats, which are always present, attacks only exist when a specific act may cause a loss. For example, the threat of damage from a thunderstorm is present throughout the summer in many places, but an attack and its associated risk of loss only exist for the duration of an actual thunderstorm.

Major Types of Attacks used Against Controlled Systems

The following sections discuss each of the major types of attacks used against controlled systems.

1. **Malicious Code :** The malicious code attack includes the execution of viruses, worms, Trojan horses, and active Web scripts with the intent to destroy or steal information. The state-of-the-art malicious code attack is the polymorphic, or multivector, worm. These attack programs use up to six known attack vectors to exploit a variety of vulnerabilities in commonly found information system devices.
2. **Hoaxes** : A more devious attack on computer systems is the transmission of a virus hoax with a real virus attached. When the attack is masked in a seemingly legitimate message, unsuspecting users more readily distribute it. Even though these users are trying to do the right thing to avoid infection, they end up sending the attack on to their coworkers and friends and infecting many users along the way.
3. **Back Doors :** Using a known or previously unknown and newly discovered access mechanism, an attacker can gain access to a system or network resource through a back door. Sometimes these entries are left behind by system designers or maintenance staff, and thus are called trap doors.34 A trap door is hard to detect, because very often the programmer who puts it in place also makes the access exempt from the usual audit logging features of the system.
4. **Password Crack :** Attempting to reverse-calculate a password is often called cracking. A cracking attack is a component of many dictionary attacks (to be covered shortly). It is used when a copy of the Security Account Manager (SAM) data file, which contains hashed representation of the user's password, can be obtained. A password can be hashed using the same algorithm and compared to the hashed results. If they are the same, the password has been cracked.

5. **Brute Force :** The application of computing and network resources to try every possible password combination is called a brute force attack. Since the brute force attack is often used to obtain passwords to commonly used accounts, it is sometimes called a password attack. If attackers can narrow the field of target accounts, they can devote more time and resources to these accounts. That is one reason to always change the manufacturer's default administrator account names and passwords.

   Password attacks are rarely successful against systems that have adopted the manufacturer's recommended security practices. Controls that limit the number of unsuccessful access attempts allowed per unit of elapsed time are very effective against brute force attacks.

6. **Dictionary** : The dictionary attack is a variation of the brute force attack which narrows the field by selecting specific target accounts and using a list of commonly used passwords (the dictionary) instead of random combinations. Organizations can use similar dictionaries to disallow passwords during the reset process and thus guard against easy-to-guess passwords. In addition, rules requiring numbers and/or special characters in passwords make the dictionary attack less effective.

7. **Denial-of-Service (DoS) and Distributed :** Denial-of-Service (DDoS) In a denial-of-service (DoS) attack, the attacker sends a large number of connection or information requests to a target. So many requests are made that the target system becomes overloaded and cannot respond to legitimate requests for service. The system may crash or simply become unable to perform ordinary functions. A distributed denialof-service (DDoS) is an attack in which a coordinated stream of requests is launched against a target from many locations at the same time.

   Most DDoS attacks are preceded by a preparation phase in which many systems, perhaps thousands, are compromised. The compromised machines are turned into zombies, machines that are directed remotely (usually by a transmitted command) by the attacker to participate in the attack. DDoS attacks are the most difficult to defend against, and there are presently no controls that any single organization can apply. There are, however, some cooperative efforts to enable DDoS defenses among groups of service providers; among them is the Consensus Roadmap for Defeating Distributed Denial of Service Attacks.

8. **Spoofing** : Spoofing is a technique used to gain unauthorized access to computers, wherein the intruder sends messages with a source IP address that has been forged to indicate that the messages are coming from a trusted host. To engage in IP spoofing, hackers use a variety of techniques to obtain trusted IP addresses, and then modify

the packet headers to insert these forged addresses. Newer routers and firewall arrangements can offer protection against IP spoofing.

9. **Man-in-the-Middle :** In the well-known man-in-the-middle or TCP hijacking attack, an attacker monitors (or sniffs) packets from the network, modifies them, and inserts them back into the network. This type of attack uses IP spoofing to enable an attacker to impersonate another entity on the network. It allows the attacker to eavesdrop as well as to change, delete, reroute, add, forge, or divert data. A variant of TCP hijacking, involves the interception of an encryption key exchange, which enables the hacker to act as an invisible man-in-the-middle—that is, an eavesdropper—on encrypted communications.

10. **Spam :** Spam is unsolicited commercial e-mail. While many consider spam a trivial nuisance rather than an attack, it has been used as a means of enhancing malicious code attacks. In March 2002, there were reports of malicious code embedded in MP3 files that were included as attachments to spam.40 The most significant consequence of spam, however, is the waste of computer and human resources. Many organizations attempt to cope with the flood of spam by using e-mail filtering technologies. Other organizations simply tell the users of the mail system to delete unwanted messages.

11. **Mail Bombing** : Another form of e-mail attack that is also a DoS is called a mail bomb, in which an attacker routes large quantities of e-mail to the target. This can be accomplished by means of social engineering (to be discussed shortly) or by exploiting various technical flaws in the Simple Mail Transport Protocol (SMTP). The target of the attack receives an unmanageably large volume of unsolicited e-mail. By sending large e-mails with forged header information, attackers can take advantage of poorly configured e-mail systems on the Internet and trick them into sending many e-mails to an address chosen by the attacker. If many such systems are tricked into participating in the event, the target e-mail address is buried under thousands or even millions of unwanted e-mails.

12. **Sniffers** : A sniffer is a program or device that can monitor data traveling over a network. Sniffers can be used both for legitimate network management functions and for stealing information. Unauthorized sniffers can be extremely dangerous to a network's security, because they are virtually impossible to detect and can be inserted almost anywhere. This makes them a favorite weapon in the hacker's arsenal. Sniffers often work on TCP/IP networks, where they're sometimes called packet sniffers. Sniffers add risk to the network, because many systems and users send information on local networks in clear text. A sniffer program shows all the data going by,

including passwords, the data inside files—such as word-processing documents—and screens full of sensitive data from applications.

13. **Social Engineering :** In the context of information security, social engineering is the process of using social skills to convince people to reveal access credentials or other valuable information to the attacker. There are several social engineering techniques, which usually involve a perpetrator posing as a person higher in the organizational hierarchy than the victim. To prepare for this false representation, the perpetrator may have used social engineering tactics against others in the organization to collect seemingly unrelated information that, when used together, makes the false representation more credible.

14. **Pharming** : Pharming is "the redirection of legitimate Web traffic (e.g., browser requests) to an illegitimate site for the purpose of obtaining private information. Pharming often uses Trojans, worms, or other virus technologies to attack the Internet browser's address bar so that the valid URL typed by the user is modified to that of the illegitimate Web site. Pharming may also exploit the Domain Name System (DNS) by causing it to transform the legitimate host name into the invalid site's IP address; this form of pharming is also known as DNS cache poisoning.

15. **Timing Attack** : A timing attack explores the contents of a Web browser's cache and stores a malicious cookie on the client's system. The cookie (which is a small quantity of data stored by the Web browser on the local system, at the direction of the Web server) can allow the designer to collect information on how to access password-protected sites. Another attack by the same name involves the interception of cryptographic elements to determine keys and encryption algorithms

1.5.4 Secure Software Development

Systems consist of hardware, software, networks, data, procedures, and people using the system. Many of the information security issues described in this chapter have their root cause in the software elements of the system. Secure systems require secure, or at least securable, software. The development of systems and the software they use is often accomplished using a methodology, such as the systems development life cycle (SDLC).

Many organizations recognize the need to include planning for security objectives in the SDLC they use to create systems, and have put in place procedures to create software that is more able to be deployed in a secure fashion. This approach to software development is known as software assurance, or SA.

Software Assurance and the SA Common Body of Knowledge

The organizations are increasingly working to build security into the systems development life cycle, to prevent security problems before they begin. A national effort is underway to create a common body of knowledge focused on secure software development.

The U.S. Department of Defense (DoD) launched a Software Assurance Initiative in 2003. This initial process was led by Joe Jarzombek and was endorsed and supported by the Department of Homeland Security (DHS), which joined the program in 2004. This program initiative resulted in the publication of the Secure Software Assurance (SwA) Common Body of Knowledge (CBK).

A working group drawn from industry, government, and academia was formed to examine two key questions:

1. What are the engineering activities or aspects of activities that are relevant to achieving secure software?
2. What knowledge is needed to perform these activities or aspects?

Based on the findings of this working group, and a host of existing external documents and standards, the SwA CBK was developed and published to serve as a guideline. While this work has not yet been adopted as a standard or even a policy requirement of government agencies, it serves as a strongly recommended guide to developing more secure applications. The SwA CBK, which is a work in progress, contains the following sections:

1. Nature of Dangers
2. Fundamental Concepts and Principles
3. Ethics, Law, and Governance
4. Secure Software Requirements
5. Secure Software Design
6. Secure Software Construction
7. Secure Software Verification, Validation, and Evaluation
8. Secure Software Tools and Methods
9. Secure Software Processes
10. Secure Software Project Management
11. Acquisition of Secure Software
12. Secure Software Sustainment.

The following sections provides insight into the stages that should be incorporated into the software SDLC.

Software Design Principles

Good software development should result in a finished product that meets all of its design specifications. Information security considerations are a critical component of those specifications,though that has not always been true.

Leaders in software development J. H. Saltzer and M. D. Schroeder note that article, The protection of information in computer systems [...and] the usefulness of a set of protection mechanisms depends upon the ability of a system to prevent security violations.

This statement could be about software development in the early part of the 21st century, but actually dates back to 1975, before information security and software assurance became critical factors for many organizations. In this same article, the authors provide insight into what are now commonplace security principles:

1. **Economy of mechanism:** Keep the design as simple and small as possible.
2. **Fail-safe defaults**: Base access decisions on permission rather than exclusion.
3. **Complete mediation:** Every access to every object must be checked for authority.
4. **Open design:** The design should not be secret, but rather depend on the possession of keys or passwords.
5. **Separation of privilege**: Where feasible, a protection mechanism should require two keys to unlock, rather than one.
6. **Least privilege:** Every program and every user of the system should operate using the least set of privileges necessary to complete the job.
7. **Least common mechanism:** Minimize mechanisms (or shared variables) common to more than one user and depended on by all users.
8. **Psychological acceptability:** It is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly.

Software Development Security Problems

Some software development problems that result in software that is difficult or impossible to deploy in a secure fashion have been identified as "deadly sins in software security." These twenty problem areas in software development (which is also called software engineering) were originally categorized by John Viega, upon request of Amit

Youran, who at the time was the Director of the Department of Homeland Security's National Cyber Security Division.

These problem areas are described in the following sections.

1. **Buffer Overruns :** Buffers are used to manage mismatches in the processing rates between two entities involved in a communication process. A **buffer overrun** (or **buffer overflow**) is an application error that occurs when more data is sent to a program buffer than it is designed to handle. During a buffer overrun, an attacker can make the target system execute instructions, or the attacker can take advantage of some other unintended consequence of the failure. Sometimes this is limited to a denial-of-service attack. In any case, data on the attacked system loses integrity.

2. **Command Injection :** Command injection problems occur when user input is passed directly to a compiler or interpreter. The underlying issue is the developer's failure to ensure that command input is validated before it is used in the program.

3. **Cross-site Scripting :** Cross site scripting (or XSS) occurs when an application running on a Web server gathers data from a user in order to steal it. An attacker can use weaknesses in the Web server environment to insert commands into a user's browser session, so that users ostensibly connected to a friendly Web server are, in fact, sending information to a hostile server. This allows the attacker to acquire valuable information, such as account credentials, account numbers, or other critical data. Often an attacker encodes a malicious link and places it in the target server, making it look less suspicious. After the data is collected by the hostile application, it sends what appears to be a valid response from the intended server.

4. **Failure to Handle Errors :** What happens when a system or application encounters an scenario that it is not prepared to handle? Does it attempt to complete the operation (reading or writing data or performing calculations)? Does it issue a cryptic message that only a programmer could understand? Or does it simply stop functioning? Failure to handle errors can cause a variety of unexpected system behaviors. Programmers are expected to anticipate problems and prepare their application code to handle them.

5. **Failure to Protect Network Traffic :** With the growing popularity of wireless networking comes a corresponding increase in the risk that wirelessly transmitted data will be intercepted. Most wireless networks are installed and operated with little or no protection for the information that is broadcast between the client and the network wireless access point. This is especially true of public networks found in

coffee shops, bookstores, and hotels. Without appropriate encryption (such as that afforded by WPA), attackers can intercept and view your data.

Traffic on a wired network is also vulnerable to interception in some situations. On networks using hubs instead of switches, any user can install a packet sniffer and collect communications to and from users on that network. Periodic scans for unauthorized packet sniffers, unauthorized connections to the network, and general awareness of the threat can mitigate this problem.

6. **Failure to Store and Protect Data Securely :** Storing and protecting data securely is a large enough issue to be the core subject of this entire text. Programmers are responsible for integrating access controls into, and keeping secret information out of, programs. Access controls, the subject of later chapters, regulate who, what, when, where, and how individuals and systems interact with data. Failure to properly implement sufficiently strong access controls makes the data vulnerable. Overly strict access controls hinder business users in the performance of their duties, and as a result the controls may be administratively removed or bypassed.

   The integration of secret information—such as the "hard coding" of passwords, encryption keys, or other sensitive information—can put that information at risk of disclosure.

7. **Failure to Use Cryptographically Strong Random Numbers :** Most modern cryptosystems, like many other computer systems, use random number generators. However, a decision support system using random and pseudo-random numbers for Monte Carlo method forecasting does not require the same degree of rigor and the same need for true randomness as a system that seeks to implement cryptographic procedures. These "random" number generators use a mathematical algorithm, based on a seed value and another other system component (such as the computer clock) to simulate a random number. Those who understand the workings of such a "random" number generator can predict particular values at particular times.

8. **Format String Problems :** Computer languages often are equipped with built-in capabilities to reformat data while they're outputting it. The formatting instructions are usually written as a "format string." Unfortunately, some programmers may use data from untrusted sources as a format string.56 An attacker may embed characters that are meaningful as formatting directives (e.g., %x, %d, %p, etc.) into malicious input; if this input is then interpreted by the program as formatting directives (such as an argument to the C printf function), the attacker may be able to access information

or overwrite very targeted portions of the program's stack with data of the attacker's choosing.

9. **Neglecting Change Control :** Developers use a process known as **change control** to ensure that the working system delivered to users represents the intent of the developers. Early in the development process, change control ensures that developers do not work at cross purposes by altering the same programs or parts of programs at the same time. Once the system is in production, change control processes ensure that only authorized changes are introduced and that all changes are adequately tested before being released.

10. **Improper File Access :** If an attacker changes the expected location of a file by intercepting and modifying a program code call, the attacker can force a program to use files other than the ones the program is supposed to use. This type of attack could be used to either substitute a bogus file for a legitimate file (as in password files), or trick the system into running a malware executable. The potential for damage or disclosure is great, so it is critical to protect not only the location of the files but also the method and communications channels by which these files are accessed.

11. **Improper Use of SSL :** Programmers use Secure Sockets Layer (SSL) to transfer sensitive data, such as credit card numbers and other personal information, between a client and server. While most programmers assume that using SSL guarantees security, unfortunately they more often than not mishandle this technology. SSL and its successor, Transport Layer Security (TLS), both need certificate validation to be truly secure. Failure to use Hypertext Transfer Protocol Secure (HTTPS), to validate the certificate authority and then validate the certificate itself, or to validate the information against a certificate revocation list (CRL), can compromise the security of SSL traffic.

12. **Information Leakage :** One of the most common methods of obtaining inside and classified information is directly or indirectly from an individual, usually an employee. The World War II military poster warned that "loose lips sink ships," emphasizing the risk to naval deployments from enemy attack should the sailors, marines, or their families disclose the movements of these vessels. It was a widely-shared fear that the enemy had civilian operatives waiting in bars and shops at common Navy ports of call, just waiting for the troops to drop hints about where they were going and when. By warning employees against disclosing information, organizations can protect the secrecy of their operation.

13. **Race Conditions** A race condition is a failure of a program that occurs when an unexpected ordering of events in the execution of the program results in a conflict

over access to the same system resource. This conflict does not need to involve streams of code inside the program, since current operating systems and processor technology automatically break a program into multiple threads that can be executed simultaneously. If the threads that result from this process share any resources, they may interfere with each other.

14. **SQL Injection** SQL injection occurs when developers fail to properly validate user input before using it to query a relational database.

15. **Poor Usability** Employees prefer doing things the easy way. When faced with an "official way" of performing a task and an "unofficial way"—which is easier—they prefer the easier method. The only way to address this issue is to only provide one way—the secure way! Integrating security and usability, adding training and awareness, and ensuring solid controls all contribute to the security of information. Allowing users to default to easier, more usable solutions will inevitably lead to loss.

IMPORTANT QUESTIONS

1. What is information security? Explain about History and Critical characteristics of information?
2. Discuss briefly about NSTISSC security model.
3. What are the Components of an information system? Explain briefly about securing the components.
4. Explain about Balancing security and access in information security.
5. What is SDLC? Explain about the security SDLC.
6. What is the Need for Security? Explain about Business needs, Threats, Attacks and secure software development.