Dr. MAHALINGAM COLLEGE OF ENGINEERING AND TECHNOLOGY

Enlightening Technical Minds Estd. 1998

An Autonomous Institution (Since 2011)

Dr. MAHALINGAM
COLLEGE OF ENGINEERING AND TECHNOLOGY
Affiliated to Anna University, Chennai; Approved by AICTE ; Accredited by NAAC with Grade 'A++'
Accredited by NBA - Tier1 (Mech, Auto, Civil, EEE, ECE, E&I and CSE)
Udumalai Road, Pollachi - 642 003. Tel: 04259-236030/40/50 Fax: 04259-236070 www.mcet.in

19ITOC1004 – Cyber Law and Information Security

Unit IV - Information Security

CO4: Explain the fundamentals concepts of information security against cyber-attacks

LO1: To learn about Information security Concepts.

Prepared by

G. Keerthika

AP/IT

Unit IV - Information Security

Information Security Concepts - Critical Characteristics of Information - CNSS Security Model - Components of an Information System - Balancing Information Security and Access – The SDLC - The Security SDLC.

Information Security concepts

Access: A subject or object's ability to use, manipulate, modify, or affect another subject or object. Authorized users have legal access to a system, whereas hackers have illegal access to a system. Access controls regulate this ability.

An asset: It can be logical, such as a Web site, information, or data; or an asset can be physical, such as a person, computer system, or other tangible object. Assets, and particularly information assets, are the focus of security efforts; they are what those efforts are attempting to protect.

Attack: Attacks can be active or passive, intentional or unintentional, and direct or indirect.

- Someone casually reading sensitive information not intended for his or her use is a **passive attack.**
- A hacker attempting to break into an information system is **an intentional attack**.
- A lightning strike that causes a fire in a building is an **unintentional attack.**
- **A direct attack** is a hacker using a personal computer to break into a system.
- **An indirect attack** is a hacker compromising a system and using it to attack other systems,

Information Security concepts

Control, safeguard, or countermeasure: Security mechanisms, policies, or procedures that can successfully counter attacks, reduce risk, resolve vulnerabilities, and otherwise improve the security within an organization.

Exploit: A technique used to compromise a system. Threat agents may attempt to exploit a system or other information asset by using it illegally for their personal gain.

Exposure: A condition or state of being exposed. In information security, exposure exists when a vulnerability known to an attacker is present.

Loss: A single instance of an information asset suffering damage or unintended or unauthorized modification or disclosure. When an organization's information is stolen, it has suffered a loss.

Protection profile or security posture: The entire set of controls and safeguards, including policy, education, training and awareness, and technology, that the organization implements (or fails to implement) to protect the asset.

Information Security concepts

Risk: The probability that something unwanted will happen. Organizations must minimize risk to match their risk appetite—the quantity and nature of risk the organization is willing to accept.

Subjects and objects: A computer can be either the subject of an attack—an agent entity used to conduct the attack—or the object of an attack—the target entity.

Threat: A category of objects, persons, or other entities that presents a danger to an asset. Threats are always present and can be purposeful or undirected.

For example, hackers purposefully threaten unprotected information systems, while severe storms incidentally threaten buildings and their contents.

Threat agent: The specific instance or a component of a threat.

Vulnerability: A weaknesses or fault in a system or protection mechanism that opens it to attack or damage. Some examples of vulnerabilities are a flaw in a software package, an unprotected system port, and an unlocked door. Some

References

Text Book(s): Michael E Whitman and Herbert J Mattord, ―Principles of Information Security||, Cengage Learning, 2018. (Unit IV, V)

Reference Book(s):

Matt Bishop, ―"Computer Security Art and Science", Pearson/PHI, 2018.

Web References:

1. http://www.cyberlawsindia.net/internet-crime.html
2. http://www.computerforensicsworld.com

Thank You

19ITOC1004 – Cyber Law and Information Security

Unit IV - Information Security

CO4: Explain the fundamentals concepts of information security against cyber-attacks

LO1: To learn about Information security Concepts.

SO1:Explain about Characteristics of Information system.

Prepared by

G. Keerthika

AP/IT

Unit IV - Information Security

Information Security Concepts - Critical Characteristics of Information - CNSS Security Model - Components of an Information System - Balancing Information Security and Access – The SDLC - The Security SDLC.

Critical Characteristics of Information

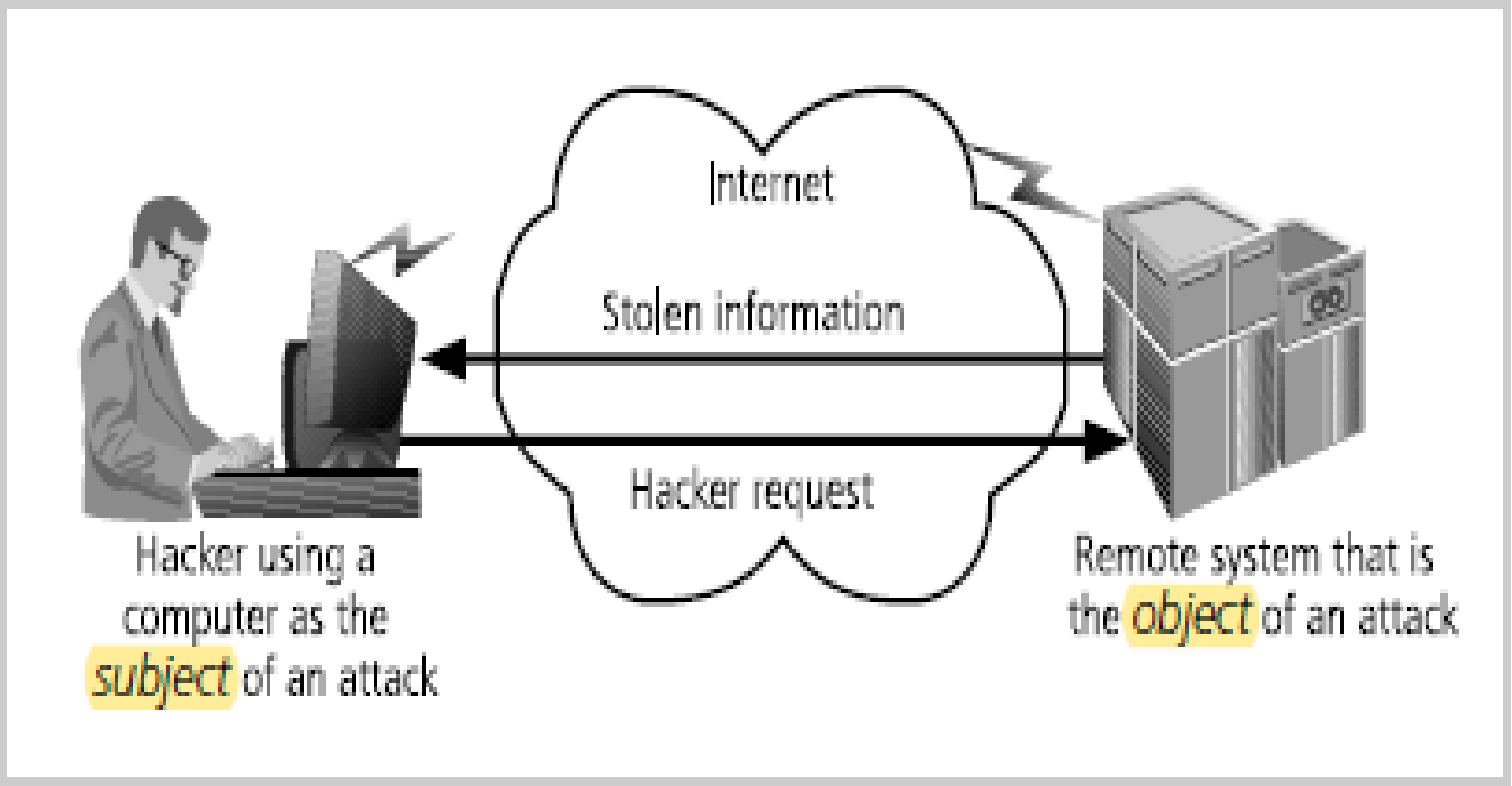

Internet
Stolen information
Hacker request
Hacker using a computer as the subject of an attack
Remote system that is the object of an attack

Figure 1-5 Computer as the Subject and Object of an Attack

Characteristics of Information

Availability: Availability enables authorized users—persons or computer systems—to access information without interference or obstruction and to receive it in the required format.

Consider, for example, Librarians protect the contents of the library so that they are available only to authorized patrons.

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.

Characteristics of Information(contd…)

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.

Example:

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.

Phishing, when an attacker attempts to obtain personal or financial information using fraudulent means, most often by posing as another individual or organization.

Characteristics of Information(contd…)

- **Confidentiality** Information has **confidentiality** when it is protected from disclosure 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.
- To protect the confidentiality of information, you can use a number of measures, including the following:
- Information classification
- Secure document storage
- Application of general security policies
- Education of information custodians and end users
- Confidentiality, like most of the characteristics of information,

Confidentiality

- The value of confidentiality of information is especially high when it is personal information about employees, customers, or patients.
- Individuals who transact with an organization expect that their personal information will remain confidential, whether the organization is a federal agency, such as the Internal Revenue Service, or a business.
- Problems arise when companies disclose confidential information. Sometimes this disclosure is intentional, but there are times when disclosure of confidential information happens by mistake.
- For example, when confidential information is mistakenly e-mailed to someone outside the organization rather than to someone inside the organization. Several cases of privacy violation are outlined in Offline: Unintentional Disclosures.

Characteristics of Information(contd…)

- **Integrity:** Information has integrity when it is whole, complete, and uncorrupted.

- The integrity of information is threatened when the information is exposed to corruption, damage, destruction, or other disruption of its authentic state.

- The key method of assuring information integrity is file hashing, in which a file is read by a special algorithm that uses the value of the bits in the file to compute a single large number called a hash value. The hash value for any combination of bits is unique.

- If a computer system performs the same hashing algorithm on a file and obtains a different number than the recorded hash value for that file, the file has been compromised and the integrity of the information is lost.

Characteristics of Information(contd…)

- **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.

Characteristics of Information(contd…)

- **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.
- For example, assume a company stores its critical customer data using an encrypted file system. An employee who has quit decides to take a copy of the tape backups to sell the customer records to the competition.

References

Text Book(s): Michael E Whitman and Herbert J Mattord, ―Principles of Information Security‖, Cengage Learning, 2018. (Unit IV, V)

Reference Book(s):

Matt Bishop, ―"Computer Security Art and Science", Pearson/PHI, 2018.

Web References:

1. http://www.cyberlawsindia.net/internet-crime.html

2. http://www.computerforensicsworld.com

Thank You

19ITOC1004 – Cyber Law and Information Security

Unit IV - Information Security

CO4: Explain the fundamentals concepts of information security against cyber-attacks

LO1: To learn about Information security Concepts.

SO2:Discuss about CNSS security model

Prepared by

G. Keerthika

AP/IT

Unit IV - Information Security

Information Security Concepts - Critical Characteristics of Information - CNSS Security Model - Components of an Information System - Balancing Information Security and Access – The SDLC - The Security SDLC.

CNSS Security Model

CNSS defines information security as the protection of information and its critical elements, including the system and hardware that use, store and transmit that information.

The NSTISSC was renamed as the Committee on National Security Systems (CNSS).

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 three dimensions.

If extrapolated, the three dimensions of each axis become a 3 3 3 cube with 27 cells representing areas that must be addressed to secure today's information systems. To ensure system security, each of the 27 areas must be properly addressed during the security process.

CNSS Security Model(contd..)

- 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.

The McCumber Cube

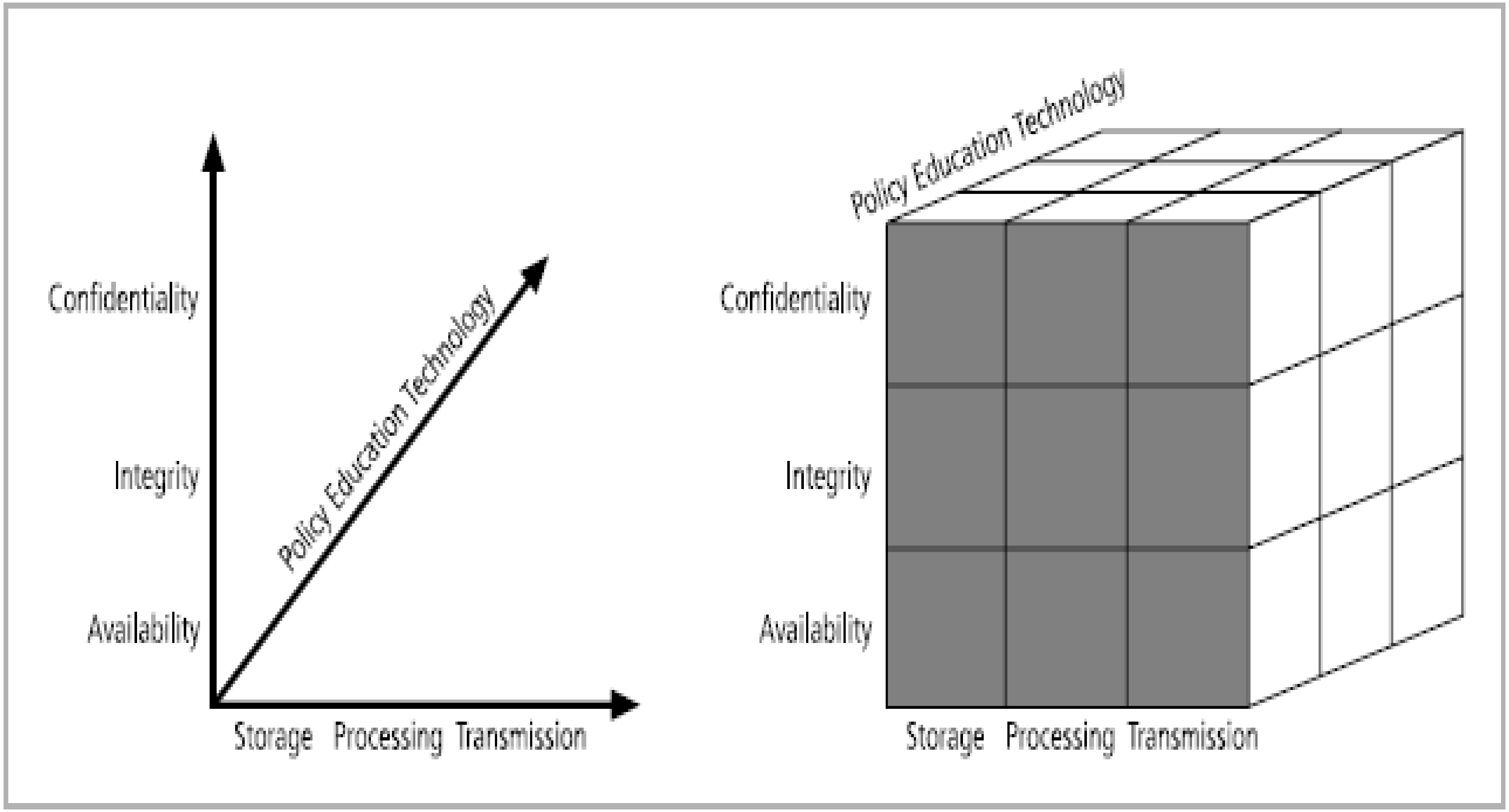


Figure 1-6 The McCumber Cube[18]

Availability: Availability enables authorized users—persons or computer systems—to access information without interference or obstruction and to receive it in the required format.

Accuracy: Information has accuracy when it is free from mistakes or errors and it has the value that the end user expects.

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.

Confidentiality: Information has confidentiality when it is protected from disclosure exposure to unauthorized individuals or systems.

Integrity: Information has integrity when it is whole, complete, and uncorrupted.

The integrity of information is threatened when the information is exposed to corruption, damage, destruction, or other disruption of its authentic state.

References

Text Book(s): Michael E Whitman and Herbert J Mattord, ―Principles of Information Security‖, Cengage Learning, 2018. (Unit IV, V)

Reference Book(s):

Matt Bishop, ―"Computer Security Art and Science", Pearson/PHI, 2018.

Web References:

1. http://www.cyberlawsindia.net/internet-crime.html
2. http://www.computerforensicsworld.com

Thank You

19ITOC1004 – Cyber Law and Information Security

Unit IV - Information Security

CO4: Explain the fundamentals concepts of information security against cyber-attacks

LO1: To learn about Information security Concepts.

SO2:Discuss about CNSS security model

Prepared by
G. Keerthika
AP/IT

Unit IV - Information Security

Information Security Concepts - Critical Characteristics of Information - CNSS Security Model - Components of an Information System - Balancing Information Security and Access – The SDLC - The Security SDLC.

CNSS Security Model

CNSS Model for University Security

The Basic objectives of CNSS/NSTISSC model are to secure data in 3 probable ways:

- Using security services
- Maintaining information states
- Setting security countermeasures

- Confidentiality-Policy and Storage: In this process, the University has certain policies and guidelines for an enrolled student and staff. All the relevant data associated is kept confidential only accessible to authorized personnel only, and a secure storage solution is provided by the University to safeguard its and student's data.
- Confidentiality-Policy and Processing: In this process, an authorized person is appointed to process data whenever required. That person must maintain the confidentiality of data and work according to university policies.

  Example: I am submitting this assignment electronically to my lecturer only.
- Confidentiality-Policy and Transmission: In this process only keeping data confidential and personal working under policies is not enough as a secure medium is required for transmission of that data when a user requests to access. The university is required to use all necessary measures to secure a transmission.
- Confidentiality-Education and Storage: Only a student enrolled subject should get the subject materials of the enrolled subject. That is the use of educational data and storage of material should be kept confidential for the actual students not all.

- Confidentiality-Education and Processing: The lecturer needs to update slides or educational materials constantly updates any new materials and sent to the subject enrolled students.
- Confidentiality-Education and transmission: Data and information related to the subject be kept secure by applying a range of measures like only enrolled students attend classes as card swap will only open lecture room doors.
- Confidentiality-Technology and Storage: The use of a database system to store and transfer data to only students that are to use.
- Confidentiality-Technology and Processing: Advance processing system as the speed of text collect data and store in the university database. This method maintains confidentiality as the system automatically integrates data from one to another form.
- Confidentiality-Technology and Transmission: The use of optical fiber to transfer data between terminals decreases chances of data being stolen, corrupt, similarly using cryptography in transmission ensures secure data.

- Integrity-Policy and Storage: Data to be uploaded in the electronic format, lecturer and university personal should check the files for corrupted or damaged. The policy to upload files should be maintained.
- Integrity-policy and processing: processing should be done by a person that is aware of university policies and is knowledgeable enough not to do mistakes in data while processing.
- Integrity-Policy and Transmission: The correct electronic data is accessible to students at a time using wired or wireless methods.
- Integrity-Education and Storage: The lecture provides up-to-date data on the university database for students to use it without any mistakes on the information they get.
- Integrity-Education and processing: Educational data and material while processing should not be altered and checked before finalizing upload to the system.

- Integrity-Education-Transmission: Only the accurate and useful data be uploaded to the student database as no incorrect data lead to a problem in university.
- Integrity-Technology and Storage: The Subject materials related to a particular subject is stored in the university database system after being checked and verified as correct and useful to students.
- Integrity-Technology and Processing: Some system or software is used to check uploading data for its authenticity.
- Integrity-Technology and transmission: The data on the university network should be correct and be available only after finalizing its integrity of use.
- Availability-Policy and Storage: The university students should get the data any time from the university database. The data should comply with all the rules and policies set by the university.

- Availability-Policy and Processing: The data on the university system should be allowed to be edited by a responsible person whenever some issues are found on available data.
- Availability-Policy and Transmission: Change in data by the lecturer on their subject should be immediately available to use by students and should not violate any rules and policies.
- Availability-Education and Storage: Material stored in the university database needs to be updated and ready to use by a student at any moment.
- Availability-Education and Processing: If any changes are to be made in lecture slides or any data. Authorized personnel needs to access it and ready to be used.

- Availability-Education and Transmission: Always ready to use data should be in the system so that students can utilize and download whenever they require.
- Availability-Technology and Storage: All necessary documents related to student store in the university database system after being checked and verified as correct, so the student can utilize and download flawlessly

References

Text Book(s): Michael E Whitman and Herbert J Mattord, ―Principles of Information Security‖, Cengage Learning, 2018. (Unit IV, V)

Reference Book(s):

Matt Bishop, ―"Computer Security Art and Science", Pearson/PHI, 2018.

Web References:

1. http://www.cyberlawsindia.net/internet-crime.html

2. http://www.computerforensicsworld.com

Thank You

19ITOC1004 – Cyber Law and Information Security

Unit IV - Information Security

CO4: Explain the fundamentals concepts of information security against cyber-attacks

LO2: Describe Information system components and models.

SO1: Explain about Components of Information system.

Prepared by

G. Keerthika

AP/IT

Unit IV - Information Security

Information Security Concepts - Critical Characteristics of Information - CNSS Security Model - Components of an Information System - Balancing Information Security and Access – The SDLC - The Security SDLC.

Components of an Information System

- 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.
- These 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.

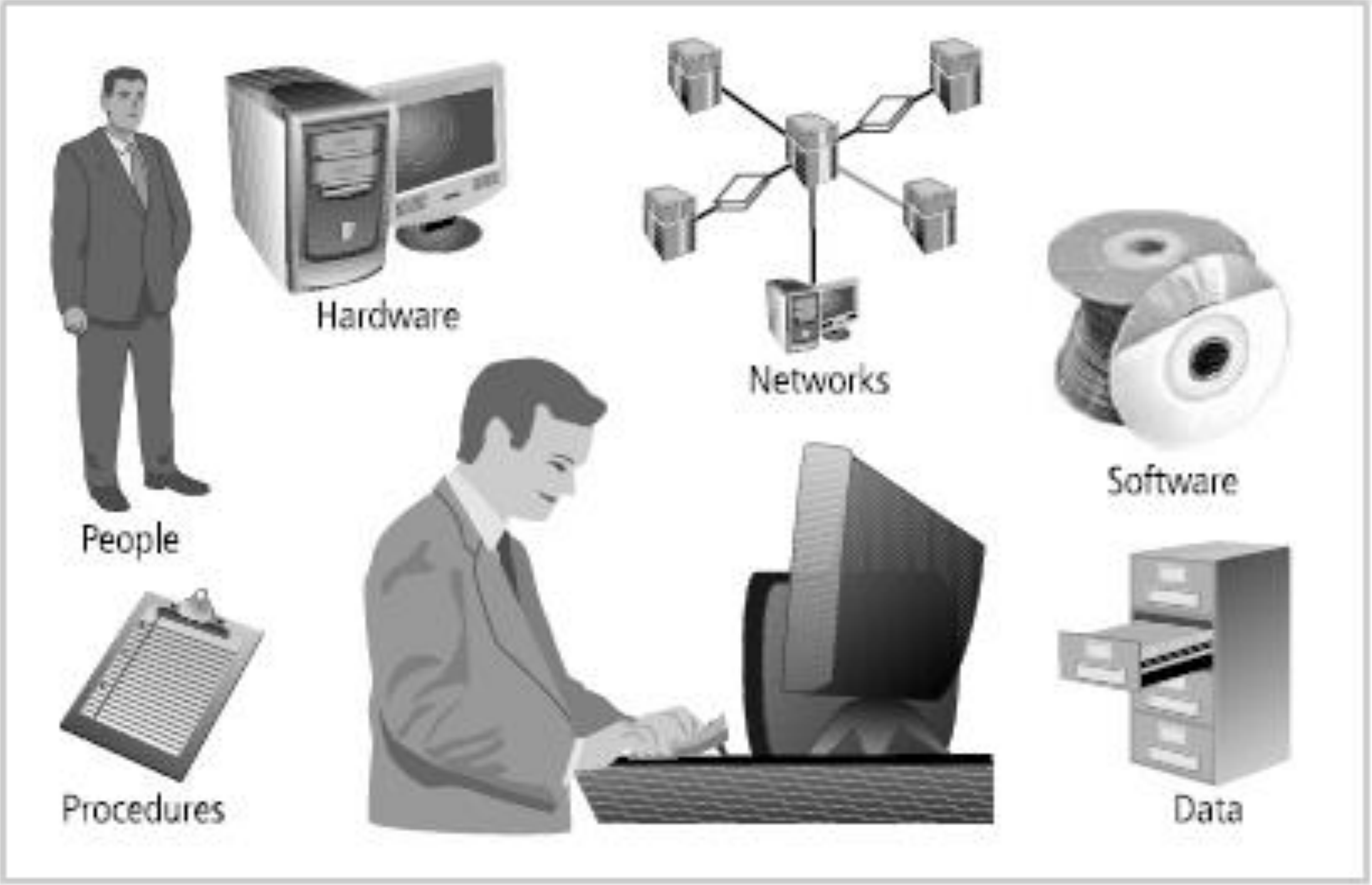


Figure 1-7 Components of an Information System

Software

- The software component of the 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.
- The information technology industry is rife with reports warning of holes, bugs, weaknesses, or other fundamental problems in software.
- In fact, many facets of daily life are affected by buggy software, from smartphones that crash to flawed automotive control computers that lead to recalls.
- Software carries the lifeblood of information through an organization. Unfortunately, software programs are often created under the constraints of project management, which limit time, cost, and manpower.
- Information security is all too often implemented as an afterthought, rather than developed as an integral component from the beginning. In this way, software programs become an easy target of accidental or intentional attacks.

Hardware

- Hardware is the physical technology that houses and executes the software, stores and transports 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 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.

Hardware

- Before September 11, 2001, laptop thefts in airports were common. A two-person team worked to steal a computer as its owner passed it through the conveyor scanning devices.
- The first perpetrator entered the security area ahead of an unsuspecting target and quickly went through. Then, the second perpetrator waited behind the target until the target placed his/her computer on the baggage scanner.
- As the computer was whisked through, the second agent slipped ahead of the victim and entered the metal detector with a substantial collection of keys, coins, and the like, thereby slowing the detection process and allowing the first perpetrator to grab the computer and disappear in a crowded walkway.

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.

people

- Though often overlooked in computer security considerations, people have always been a threat to information security.
- People can be the weakest link in an organization’s information security program.
- 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.
- Social engineering can prey on the tendency to cut corners and the common place nature of human error. It can be used to manipulate the actions of people to obtain access information about a system.

Procedure

- Another frequently overlooked component of an IS is procedures. Procedures are written instructions for accomplishing a specific task.
- When an unauthorized user obtains an organization’s procedures, this poses a threat to the integrity of the information.
- For example, a consultant to a bank learned how to wire funds by using the computer center’s procedures, which were readily available.
- By taking advantage of a security weakness (lack of authentication), this bank consultant ordered millions of dollars to be transferred by wire to his own account.
- Lax security procedures caused the loss of over ten million dollars before the situation was corrected.
- Most organizations distribute procedures to their legitimate employees so they can access the information system, but many of these companies often fail to provide proper education on the protection of the procedures.
- Educating employees about safeguarding procedures is as important as physically securing the information system.
- After all, procedures are information in their own right. Therefore, knowledge of procedures, as with all critical information, should be disseminated among members of the organization only on a need-to-know basis.

Network

- The IS component that created much of the need for increased computer and information security is networking.
- When information systems are connected to each other to form local area networks (LANs), and these LANs are connected to other networks such as the Internet, new security challenges rapidly emerge.
- The physical technology that enables network functions is becoming more and more accessible to organizations of every size.
- 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, but when computer systems are networked, this approach is no longer enough.
- Steps to provide network security are essential, as is the implementation of alarm and intrusion systems to make system owners aware of ongoing compromises.

References

Text Book(s): Michael E Whitman and Herbert J Mattord, ―Principles of Information Security‖, Cengage Learning, 2018. (Unit IV, V)

Reference Book(s):

Matt Bishop, ―"Computer Security Art and Science", Pearson/PHI, 2018.

Web References:

1. http://www.cyberlawsindia.net/internet-crime.html

2. http://www.computerforensicsworld.com

Thank You

19ITOC1004 – Cyber Law and Information Security

Unit IV - Information Security

CO4: Explain the fundamentals concepts of information security against cyber-attacks

LO2: Describe Information system components and models.

SO2:To know about balancing information security and access

Prepared by

G. Keerthika

AP/IT

Unit IV - Information Security

Information Security Concepts - Critical Characteristics of Information - CNSS Security Model - Components of an Information System - Balancing Information Security and Access – The SDLC - The Security SDLC.

Balancing Information Security and Access

- Even with the best planning and implementation, it is impossible to obtain perfect information security.
- 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 to 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.

Balancing Information Security and 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.
- 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.
- 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.

Balancing Information Security and Access

- 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.

Balancing Information Security and Access

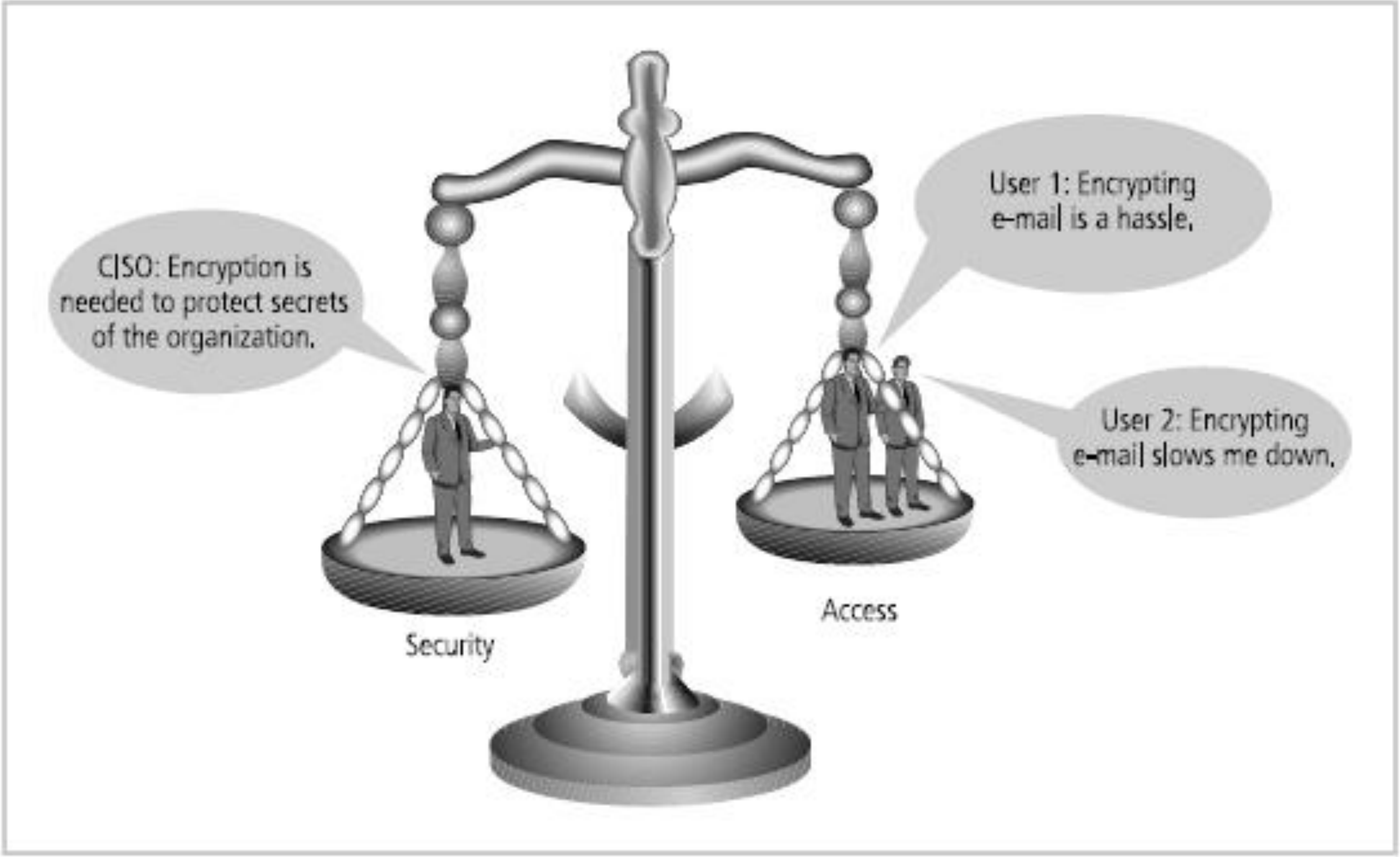

CISO: Encryption is needed to protect secrets of the organization.
User 1: Encrypting e-mail is a hassle.
User 2: Encrypting e-mail slows me down.
Security
Access

Figure 1-8 Balancing Information Security and Access

References

Text Book(s): Michael E Whitman and Herbert J Mattord, ―Principles of Information Security‖, Cengage Learning, 2018. (Unit IV, V)

Reference Book(s):

Matt Bishop, ―"Computer Security Art and Science", Pearson/PHI, 2018.

Web References:

1. http://www.cyberlawsindia.net/internet-crime.html

2. http://www.computerforensicsworld.com

Thank You

19ITOC1004 – Cyber Law and Information Security

Unit IV - Information Security

CO4: Explain the fundamentals concepts of information security against cyber-attacks

LO2: Describe Information system components and models.

SO3:Explain about SDLC model.

Prepared by

G. Keerthika

AP/IT

Unit IV - Information Security

Information Security Concepts - Critical Characteristics of Information - CNSS Security Model - Components of an Information System - Balancing Information Security and Access – The SDLC - The Security SDLC.

The 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

- 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 illustrates that each phase begins with the results and information gained from the previous phase.

Methodology and phases

- 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.
- Once the system is implemented, it is maintained (and modified) over the remainder of its operational life.
- Any information systems implementation may have multiple iterations as the cycle is repeated over time.
- Only by means of constant examination and renewal can any system, especially an information security program, perform up to expectations in the constantly changing environment in which it is placed.

Waterfall Methodology

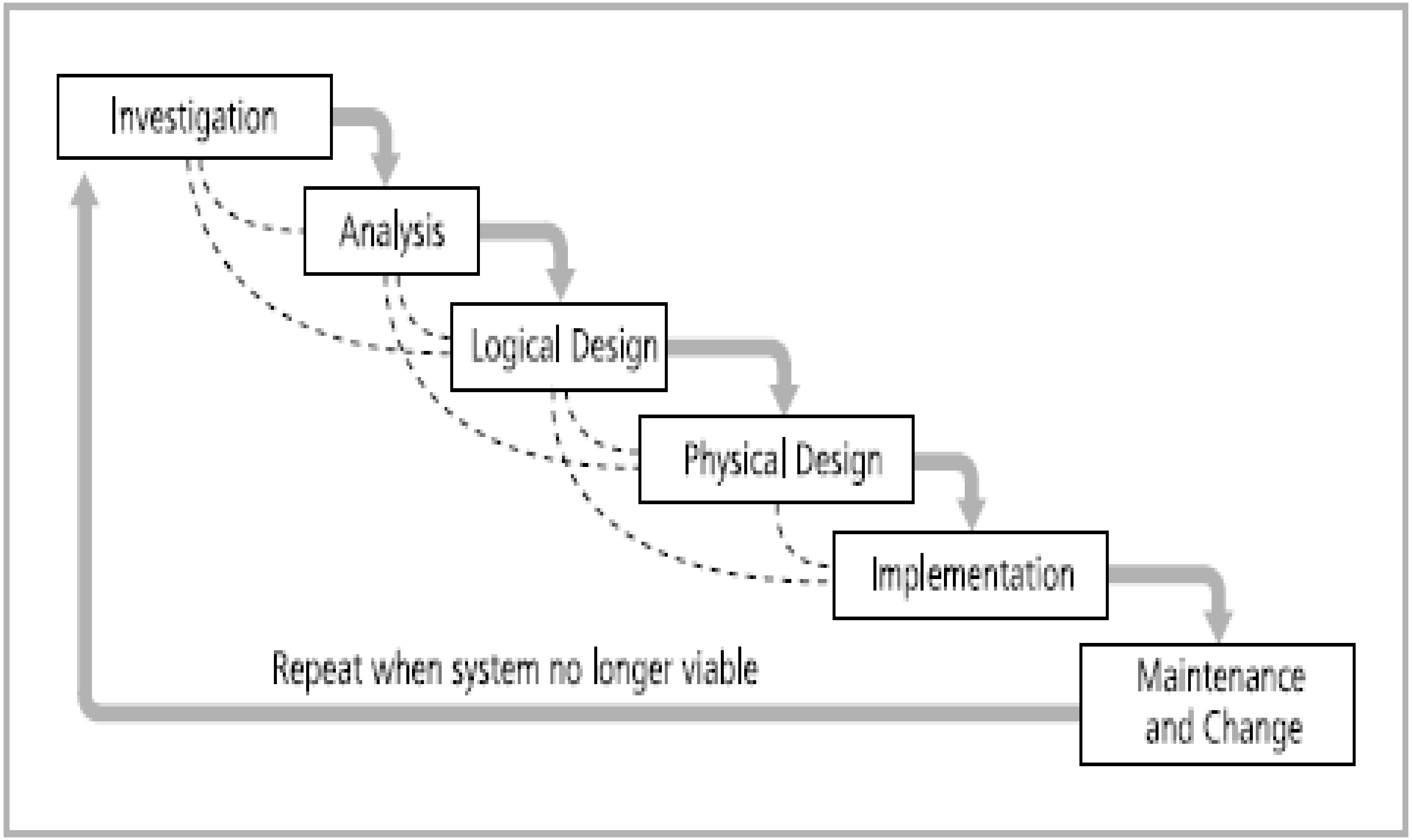


Figure 1-10 SDLC Waterfall Methodology

Investigation phase

- 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.

Analysis phase

- 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.

Logical design phase

- 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

Logical design phase

- 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.

Physical design phase

- 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.

Implementation phase

- 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.

Maintenance and change phase

- 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.

References

Text Book(s): Michael E Whitman and Herbert J Mattord, ―Principles of Information Security‖, Cengage Learning, 2018. (Unit IV, V)

Reference Book(s):

Matt Bishop, ―"Computer Security Art and Science", Pearson/PHI, 2018.

Web References:

1. http://www.cyberlawsindia.net/internet-crime.html

2. http://www.computerforensicsworld.com

Thank You

19ITOC1004 – Cyber Law and Information Security

Unit IV - Information Security

CO4: Explain the fundamentals concepts of information security against cyber-attacks

LO2: Describe Information system components and models.

SO4: To know about Security SDLC

Prepared by

G. Keerthika

AP/IT

Unit IV - Information Security

Information Security Concepts - Critical Characteristics of Information - CNSS Security Model - Components of an Information System - Balancing Information Security and Access – The SDLC - The Security SDLC.

The security SDLC

- **The investigation phase** of the SecSDLC 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 (EISP), which outlines the implementation of a security program within the organization.
- Teams of responsible managers, employees, and contractors are organized; problems are analyzed; and the 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 phase

- In the analysis phase, the documents from the investigation phase are studied. The development team conducts a preliminary analysis of existing security policies or programs, along with that of documented current threats and associated controls.
- This phase also includes an analysis of relevant legal issues that could affect the design of the security solution.
- Increasingly, privacy laws have become a major consideration when making decisions about information systems that manage personal information. Recently, many states have implemented legislation making certain computer-related activities illegal.
- A detailed understanding of these issues is vital. Risk management also begins in this stage.
- 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 phase

- The logical design phase creates and develops the blueprints for information security, and examines and implements key policies that influence later decisions.
- Also at this stage, the team plans the incident response actions to be taken in the event of partial or catastrophic loss.
- 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?

- Next, a feasibility analysis determines whether or not the project should be continued or be outsourced.

Physical design phase

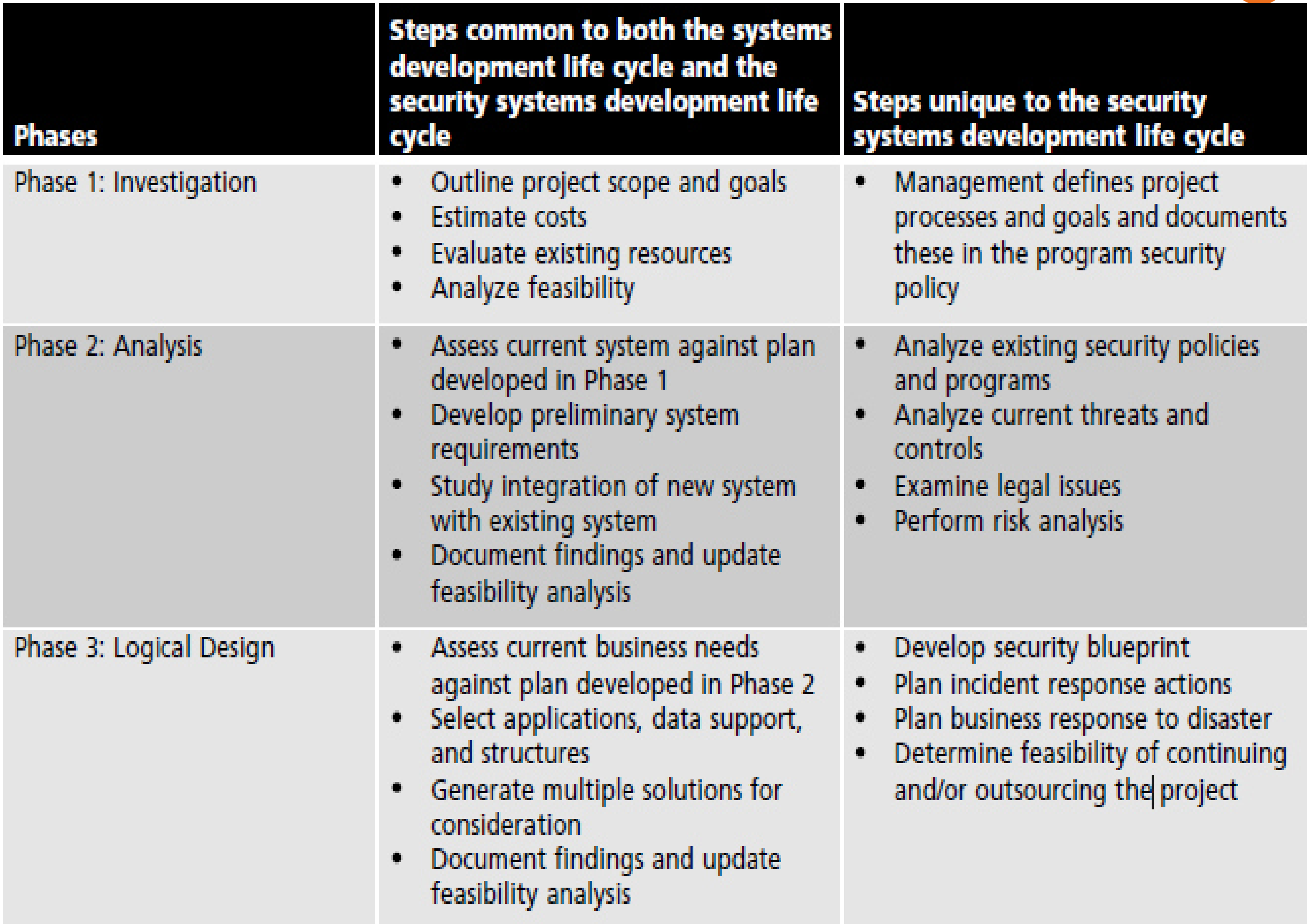
- The physical design phase evaluates the information security technology needed to support the blueprint outlined in the logical design generates alternative solutions, and determines a final design.
- The information security blueprint may be revisited to keep it in line with the changes needed when the physical design is completed.
- Criteria for determining the definition of successful solutions are also prepared during this phase. Included at this time are the designs for physical security measures to support the proposed technological solutions.
- At the end of this phase, a feasibility study determines the readiness of the organization for the proposed project, and then the champion and sponsors are presented with the design.
- At this time, all parties involved have a chance to approve the project before implementation begins.

Implementation phase

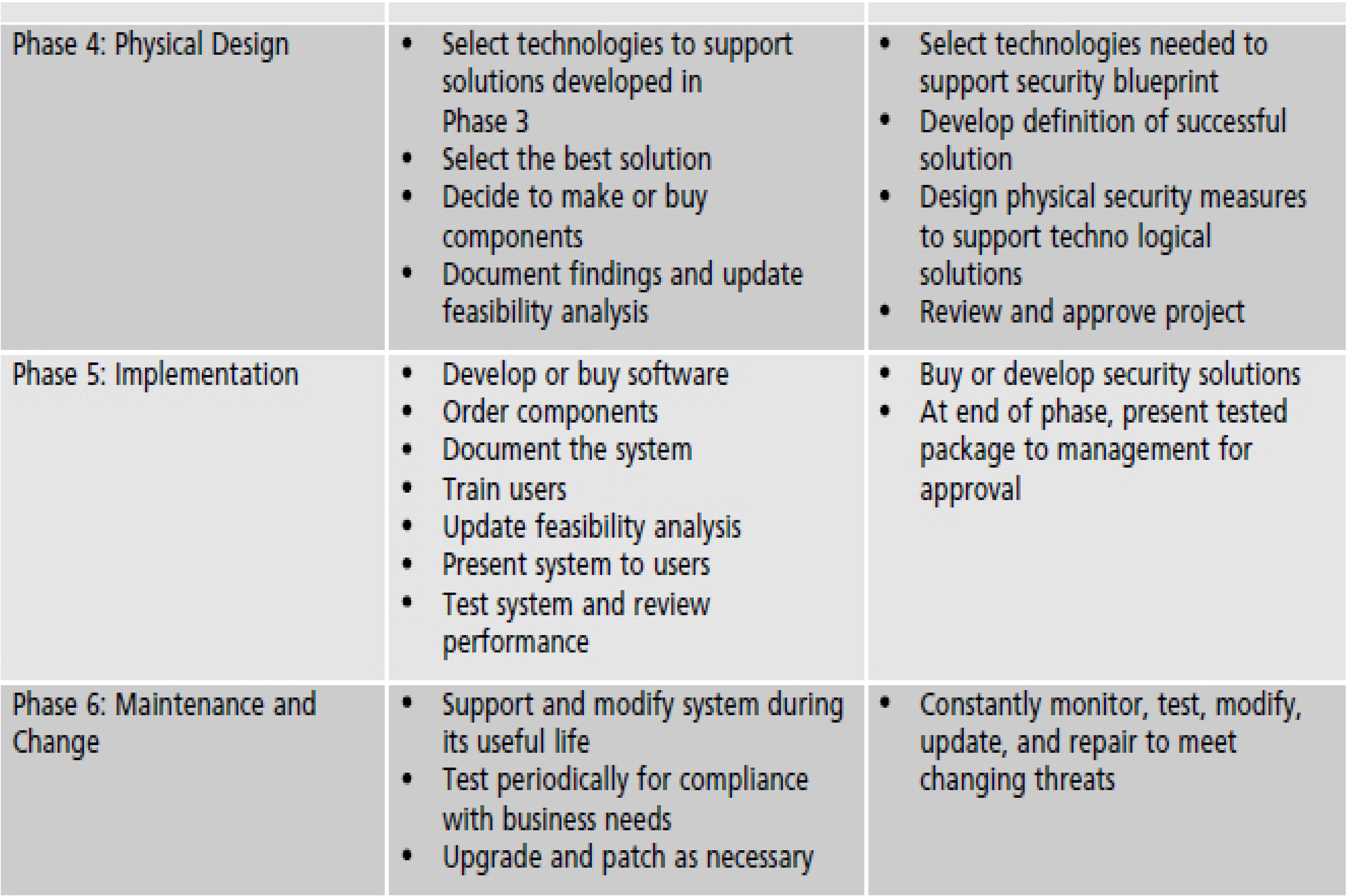
- The implementation phase in of SecSDLC is also similar to that of the traditional SDLC.
- The security solutions are acquired (made or bought), tested, implemented, and tested again.
- Personnel issues are evaluated, and specific training and education programs conducted.
- Finally, the entire tested package is presented to upper management for final approval.

Maintenance and change phase

- Maintenance and change is the last, though perhaps most important, phase, given the current ever-changing threat environment.
- Today's information security systems need constant monitoring, testing, modification, updating, and repairing.
- Applications systems developed within the framework of the traditional SDLC are not designed to anticipate a software attack that requires some degree of application reconstruction.
- In information security, the battle for stable, reliable systems is a defensive one. Often, repairing damage and restoring information is a constant effort against an unseen adversary.
- As new threats emerge and old threats evolve, the information security profile of an organization must constantly adapt to prevent threats from successfully penetrating sensitive data.
- This constant vigilance and security can be compared to that of a fortress where threats from outside as well as from within must be constantly monitored and checked with continuously new and more innovative technologies.



Phases	Steps common to both the systems development life cycle and the security systems development life cycle	Steps unique to the security systems development life cycle
Phase 1: Investigation	• Outline project scope and goals • Estimate costs • Evaluate existing resources • Analyze feasibility	• Management defines project processes and goals and documents these in the program security policy
Phase 2: Analysis	• Assess current system against plan developed in Phase 1 • Develop preliminary system requirements • Study integration of new system with existing system • Document findings and update feasibility analysis	• Analyze existing security policies and programs • Analyze current threats and controls • Examine legal issues • Perform risk analysis
Phase 3: Logical Design	• Assess current business needs against plan developed in Phase 2 • Select applications, data support, and structures • Generate multiple solutions for consideration • Document findings and update feasibility analysis	• Develop security blueprint • Plan incident response actions • Plan business response to disaster • Determine feasibility of continuing and/or outsourcing the project



Phase 4: Physical Design	- Select technologies to support solutions developed in Phase 3 - Select the best solution - Decide to make or buy components - Document findings and update feasibility analysis	- Select technologies needed to support security blueprint - Develop definition of successful solution - Design physical security measures to support techno logical solutions - Review and approve project
Phase 5: Implementation	- Develop or buy software - Order components - Document the system - Train users - Update feasibility analysis - Present system to users - Test system and review performance	- Buy or develop security solutions - At end of phase, present tested package to management for approval
Phase 6: Maintenance and Change	- Support and modify system during its useful life - Test periodically for compliance with business needs - Upgrade and patch as necessary	- Constantly monitor, test, modify, update, and repair to meet changing threats

References

Text Book(s): Michael E Whitman and Herbert J Mattord, ―Principles of Information Security‖, Cengage Learning, 2018. (Unit IV, V)

Reference Book(s):

Matt Bishop, ―"Computer Security Art and Science", Pearson/PHI, 2018.

Web References:

1. http://www.cyberlawsindia.net/internet-crime.html

2. http://www.computerforensicsworld.com

Thank You