To the unknown future reader. Thank you, because of you I have to work hard and compile these notes. The extra material was added from course books.

CS205

Information Security

These will help those who take lectures :)

Week 1 to Week 8

Created by BC180402593

Week 01 – Topic 01

Course Books

- **Principles of Information Security** 3rd Edition by Michael E. Whitman and Herbert J. Mattord
- **Computer Security: Art and Science,** Matthew Bishop
- **Cryptography and Network Security** by William Stalling 6th Edition, 2012

Learning Objectives

- Learn basic concepts of Information Security
- Develop good understanding of security, security issues, security policies, information assets, threats and Software Attacks with deep insight
- Ability to understand and plan security information system
- Knowledge gained in this course will be helpful in implementation and maintenance of security policies

Week 1

Introduction to information security

- Introduction
- History of an information security
- What is security?
- Components of information systems
- Information Flow
- Balancing the information security and access

What is Information Security?

- Information Security is the practice of defending information from
  - Unauthorized access,
  - Unauthorized use,
  - Disclosure,
  - Disruption,

  - Modification,
  - Perusal,
  - Inspection,
  - Recording
  - Destruction.
- It is a general term that can be used regardless of the form the data may take.

Introduction

Security is the prevention of certain types of intentional actions from occurring in a system.

  - These potential actions are ***threats***.
  - Threats that are carried out are ***attacks***.
  - Intentional attacks are carried out by an ***attacker***.
  - Objects of attacks are ***assets***.

Goals of Security

1. **Prevention**
   - Prevent attackers from violating security policy
2. **Detection**
   - Detect attackers' violation of security policy
3. **Recovery**
   - Stop attack, assess and repair damage
4. **Survivability**
   - Continue to function correctly even if attack succeeds

Security Measures

Technology

  - Hardware/software used to ensure security.

Policy and practice

  - Security requirements and activities.

Education, training, and awareness

  - Understanding of threats and vulnerabilities and how to protect against them.

Week 01 – Topic 02

Introduction to information security

- Introduction
- History of an information security
- What is security
- Components of information systems
- Information Flow
- Balancing the information security and access

The History of Information Security

- Began immediately after the first mainframes were developed.

Earlier versions of the German code machine Enigma were first broken by the Poles in the 1930s. The British and Americans managed to break later, more complex versions during World War II. The increasingly complex versions of the Enigma, especially the submarine or *Unterseeboot* version of the Enigma, caused considerable anguish to Allied forces before finally being cracked. The information gained from decrypted transmissions was used to anticipate the actions of German armed forces. "Some ask why, if we were reading the Enigma, we did not win the war earlier. One might ask, instead, when, if ever, we would have won the war if we hadn't read it."[1]

- Code-breaking during World War II. (Machine enigma)
- Physical controls to limit access to sensitive military locations to authorized personnel: badges, keys, and facial recognition.
- One of 1st documented problems
  - Happened in Early 1960s
  - It was not physical in nature.
  - Software glitch caused the accidental file switch

- The Entire password file
- printed on every output file

The 1960s

- *Advanced Research Procurement Agency* (ARPA) began to examine feasibility of redundant networked communications.
- *Larry Roberts* developed ARPANET.
- ARPANET is the first Internet.

The 1970s and 80s

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

R-609 Report

- Information security began with Rand Report R-609 (paper that started the study of computer security)
- Scope of computer security grew from physical security to include:
  - Safety of data
  - Limiting unauthorized access to data
  - Involvement of personnel from multiple levels of an organization
    - First identified role of management and policy issues.
- **MULTICS:** First OS containing security in its core functions.

The 1990s

- Networks of computers became more common; so too did the need to interconnect networks
- Internet became first manifestation of a global network of networks
- In early Internet deployments, security was treated as a low priority

2000 to Present

- The Internet brings millions of computer networks into communication with each other—many of them unsecured.
- This resulted in realization of information security, its importance and its use.

Week 01 – Topic 03

What is Security?

- "The quality or state of being secure-to be free from danger."

What is Information Security?

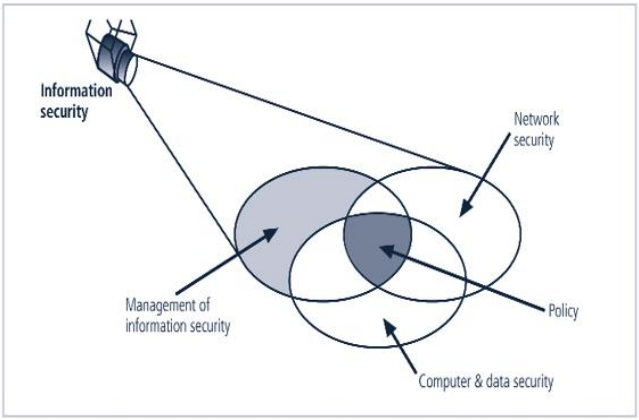
- The Committee on National Security Systems (CNSS) defines information security as the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information.

How to Achieve Security?

A successful organization should have multiple layers of security in place:

- **Physical security**, to protect physical items, objects, or areas from unauthorized access and misuse.
- **Personnel security**, to protect the individual or group of individuals who are authorized to access the organization and its operations – Human Beings.
- **Operations security**, to protect the details of a particular operation or series of Activities.
- **Communications security**, to protect communications media, technology, and content.
- **Network security**, to protect networking components, connections, and contents.
- **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.

Components of Information Security



CIA 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 is the concealment of information or resources. The need for keeping information secret arises from the use of computers in institutions with sensitive information such as government and industry. For example, military and civilian institutions in the government often restrict access to information to those who need that information.

Integrity refers to the trustworthiness of data or resources, and it is usually phrased in terms of preventing improper or unauthorized change. Integrity includes *data integrity* (the content of the information) and *origin integrity* (the source of the data, often called authentication). The source of the information may bear on its accuracy and credibility and on the trust that people place in the information.

Availability refers to the ability to use information or resources. Availability is an important aspect of reliability as well as of system design because an unavailable system is at least as bad as no system at all. The aspect of availability that is relevant to security is that someone may deliberately arrange to deny access to data or to a service by making it unavailable or unusable.

The C.I.A. triangle model no longer adequately addresses the constantly changing environment.

Key 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.

- **Asset:** The organizational resource that is being protected. An asset 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:** An intentional or unintentional act that can cause damage to or otherwise compromise information and/or the systems that support it. 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.

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

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

- **Exploit:** A technique used to compromise a system. This term can be a verb or a noun. Threat agents may attempt to exploit a system or other information asset by using it illegally for their personal gain. Or, an exploit can be a documented process to take advantage of a vulnerability or exposure, usually in software, that is either inherent in the software or is created by the attacker. Exploits make use of existing software tools or custom-made software components.

- **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 / security posture:** The entire set of controls and safeguards, including policy, education, training and awareness, and technology, that organization implements (or fails to implement) to protect the asset. The terms are sometimes used interchangeably with the term *security program*, although the security program often comprises managerial aspects of security, including planning, personnel, and subordinate programs.

- **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 that is under attack.* A computer can be both the subject and object of an attack, when, for example, it is compromised by an attack (object), and is then used to attack other systems (subject).

- **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.

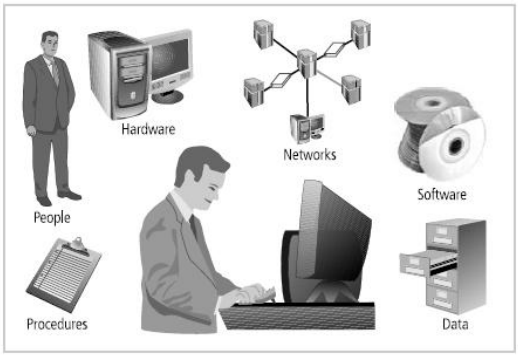
- **Threat agent:** Threat agent: The specific instance or a component of a threat. For example, all hackers in the world present a collective threat, while Kevin Mitnick, who was convicted for hacking into phone systems, is a specific threat agent. Likewise, a lightning strike, hailstorm, or tornado is a threat agent that is part of the threat of severe storms.

- **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 well-known vulnerabilities have been examined, documented, and published; others remain latent (or undiscovered).

Week 01 – Topic 04

Components of Information System

Information System (IS) is much more than computer hardware; it is entire set of software, hardware, data, people, procedures, and networks necessary to use information as a resource 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.



1. Software
2. Hardware
3. Data
4. People
5. Procedures
6. Networks

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.

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 commonplace nature of human error. It can be used to manipulate the actions of people to obtain access information about a system.

Procedures

Another frequently overlooked component of an Information System (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. 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.

Networks

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.

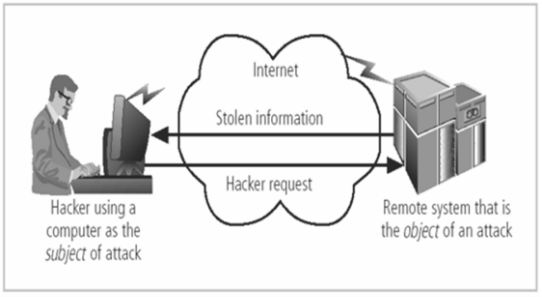
Types of attack

Computer can be subject of an attack and/or the object of an attack

- When the subject of an attack, computer is used as an active tool to conduct attack
- When the object of an attack, computer is the entity being attacked

There are 2 types of attack

- Direct - Hacker uses their computer to break into a system.
- Indirect - System is compromised and used to attack other systems.



Computer as the Subject and Object of an Attack

Week 01 – Topic 05

Information flow

- Path taken by data from sender to receiver. Although access controls can constrain the rights of a user, they cannot constrain the flow of information through a system.

Characteristics of Information

The value of information comes from the characteristics it possesses. When a characteristic of information changes, the value of that information either increases, or, more commonly, decreases. Some characteristics affect information's value to users more than others do. This can depend on circumstances. Each critical characteristic of information—that is, the expanded form of C.I.A. triangle—is defined below.

1. Timeliness
2. Availability
3. Accuracy
4. Authenticity
5. Confidentiality
6. Integrity
7. Utility
8. Possession

Timeliness

Timeliness of information can be a critical factor, because information loses much or all of its value when it is delivered too late. Though information security professionals and end users share an understanding of the characteristics of information, tensions can arise when the need to secure the information from threats conflicts with the end users' need for unhindered access to the information. For instance, end users may perceive a tenth-of-a-second delay in the computation of data to be an unnecessary annoyance. Information security professionals, however, may perceive that tenth of a second as a minor delay that enables an important task, like data encryption.

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, research libraries that require identification before entrance. Librarians protect the contents of the library so that they are available only to authorized patrons. The librarian must accept a patron's identification before that patron has free access to the book stacks. Once authorized patrons have access to the contents of the stacks, they expect to find the information they need available in a useable format and familiar language, which in this case typically means bound in a book and written in English.

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.

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.

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. 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, is interdependent with other characteristics and is most closely related to the characteristic known as privacy. 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.

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. Corruption can occur while information is being stored or transmitted. Many computer viruses and worms are designed with the explicit purpose of corrupting data. For this reason, a key method for detecting a virus or worm is to look for changes in file integrity as shown by the size of the file. Another 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. Information integrity is the cornerstone of information systems, because information is of no value or use if users cannot verify its integrity.

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.

Possession

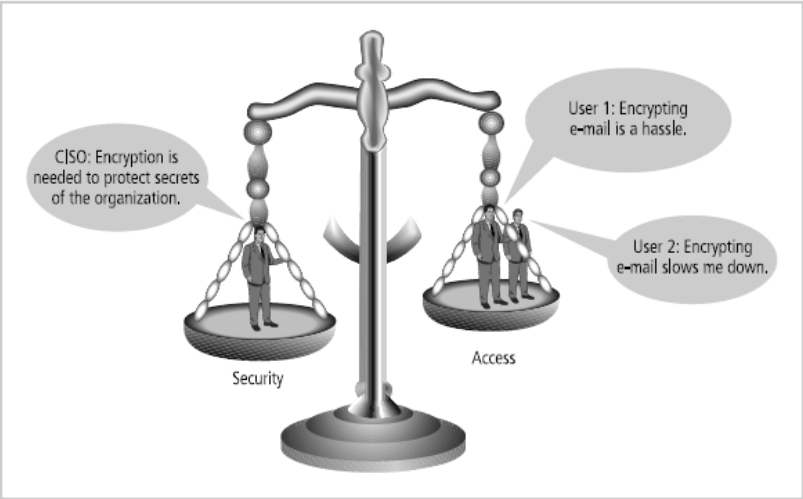
The possession of information is the quality or state of ownership or control. Information is said to be in one's possession if one obtains it, independent of format or other characteristics. While a breach of confidentiality always results in a breach of possession, a breach of possession does not always 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. The removal of the tapes from their secure environment is a breach of possession. But, because the data is encrypted, neither the employee nor anyone else can read it without the proper decryption methods; therefore, there is no breach of confidentiality. Today, people caught selling company secrets face increasingly stiff fines with the likelihood of jail time. Also, companies are growing more and more reluctant to hire individuals who have demonstrated dishonesty in their past.

Week 01 – Topic 06

Balancing Information Security and Access

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

Week 02 – Topic 01

ITU-T X.800 Security Architecture for OSI

The OSI Security Architecture is a framework that provides a systematic way of defining the requirements for security and characterizing the approaches to satisfying those requirements. The document defines security attacks, mechanisms, and services, and the relationships among these categories.

ITU-T: *International Telecommunication Union Telecommunication Standardization Sector*

OSI: *Open Systems Interconnections*

Security Services

Requirements X.800 defines security services in following categories.

1. Authentication:

The authentication service is concerned with assuring that a communication is authentic:

- The recipient of the message should be sure that the message came from the source that it claims to be
- All communicating parties should be sure that the connection is not interfered with by unauthorized party.

Example: consider a person, using online banking service. Both the user and the bank should be assured in identities of each other.

2. Access control:

The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).

3. Data confidentiality:

Protection of data from unauthorized disclosure. It includes:

- Connection confidentiality
- Connectionless confidentiality
- Selective field confidentiality
- Traffic-Flow Confidentiality

4. Data Integrity:

The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).

5. Nonrepudiation:

Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

Nonrepudiation can be related to

- **Origin**: proof that the message was sent by the specified party
- **Destination**: proof that the message was received by the specified party

Example: Imagine a user of online banking who has made a transaction, but later denied that. How the bank can protect itself in such situation?

6. Availability service:

The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system (i.e., a system is available if it provides services according to the system design whenever users request them).

Security mechanisms: are used to implement security services. They include (X.800):

- **Encipherment:**

The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.

- **Digital signature:**

Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery (e.g., by the recipient).

- **Access Control:**

A variety of mechanisms that enforce access rights to Resources.

- **Data Integrity:**

A variety of mechanisms used to assure the integrity of a data unit or stream of data units.

- **Authentication Exchange:**

A mechanism intended to ensure the identity of an entity by means of information exchange.

- **Traffic Padding:**

The insertion of bits into gaps in a data stream to frustrate eavesdropper's traffic analysis attempts.

- **Routing Control:**

Enables selection of particular physically secure Routes for certain data and allows routing changes, especially when a breach of security is suspected.

- **Notarization:**

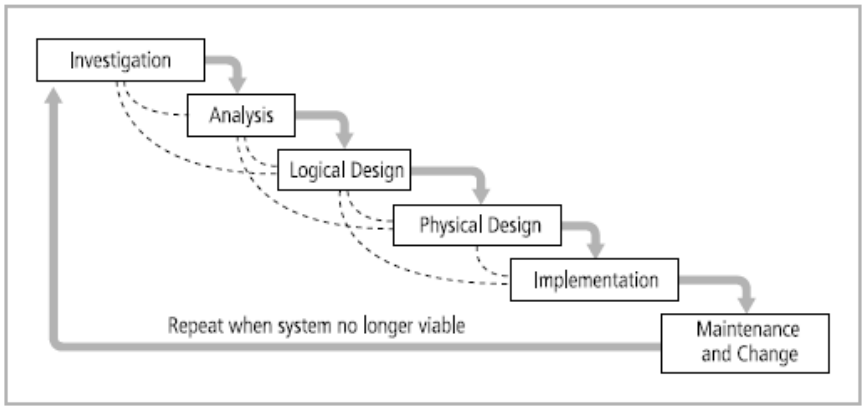
The use of a trusted third party to assure certain properties of a data exchange.

Week 02 – Topic 02

The Systems Development Life Cycle

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. The waterfall model pictured in Figure illustrates that each phase begins with the results and information gained from the previous phase. At the end of each phase comes a structured review or reality check, during which the team determines if the project should be continued, discontinued, outsourced, postponed, or returned to an earlier phase depending on whether the project is proceeding as expected and on the need for additional expertise, organizational knowledge, or other resources. 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.

The following sections describe each phase of the traditional SDLC.



1. Investigation

The first phase, investigation, is the most important. What problem is the system being developed to solve? 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.

Week 02 – Topic 03

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

Investigation

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

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. 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

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

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

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

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.

SDLC and SecSDLC Phase Summary

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	• Select technologies needed to support security blueprint

	• Decide to make or buy components • Document findings and update feasibility analysis	• 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

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

Week 03 – Topic 01

Introduction:
In general, people elect to trade some aspects of personal freedom for social order. The rules the members of a society create to balance the individual rights to self-determination against the needs of the society as a whole are called **laws**. Laws are rules that mandate or prohibit certain behavior; they are drawn from **ethics**, which define socially acceptable behaviors. The key difference between laws and ethics is that laws carry the authority of a governing body, and ethics do not. Ethics in turn are based on **cultural mores**: the fixed moral attitudes or customs of a particular group. Some ethical standards are universal. For example, murder, theft, assault, and arson are actions that deviate from ethical and legal codes throughout the world.

Organizational Liability:
What if an organization does not demand or even encourage strong ethical behavior from its employees? What if an organization does not behave ethically? Even if there is no breach of criminal law, there can still be liability. Liability is the **legal obligation** of an entity that extends beyond criminal or contract law; it includes the legal obligation to make restitution, or to compensate for wrongs committed. The bottom line is that if an employee, acting with or without the authorization of the employer, performs an illegal or unethical act that causes some degree of harm, the employer can be held financially liable for that action. An organization increases its liability if it refuses to take measures known as **due care**.

Organizational Responsibilities for Due Care and Due Diligence:
Due care standards are met when an organization makes sure that every employee knows what is acceptable or unacceptable behavior, and knows the consequences of illegal or unethical actions. *Due diligence* requires that an organization make a valid effort to protect others and continually maintains this level of effort. Given the Internet's global reach, those who could be injured or wronged by an organization's employees could be anywhere in the world.

Policy vs Law
Within an organization, information security professionals help maintain security via the establishment and enforcement of policies. These policies—guidelines that describe *acceptable* and *unacceptable* employee behaviors in the workplace—function as organizational laws, complete with penalties, judicial practices, and sanctions to require compliance. Because these policies function as laws, they must be crafted and implemented with the same care to ensure that they are complete, appropriate, and fairly applied to everyone in the workplace. The difference between a policy and a law (External legal requirements), however, is that ignorance of a policy is an acceptable defense.

Types of Law
Civil law comprises a wide variety of laws that govern a nation or state and deal with the relationships and conflicts between organizational entities and people.
Criminal law addresses activities and conduct harmful to society, and is actively enforced by the state. Law can also be categorized as private or public.
Private law encompasses family law, commercial law, and labor law, and regulates the relationship between individuals and organizations.
Public law regulates the structure and administration of government agencies and their relationships with citizens, employees, and other governments. Public law includes criminal, administrative, and constitutional law.

Week 03 – Topic 02

Law and ethics in information security

Laws
- Rules that mandate or prohibit certain behavior in society.
- Carry the sanctions of governing authority.

Ethics
- Define socially acceptable behaviors.
- Universally recognized examples include murder, theft, assault, and arson.

Key U.S. Laws of Interest to Information Security Professionals

Area	Act	Date	Description
Telecommunications	Telecommunications Deregulation and Competition Act of 1996—Update to Communications Act of 1934 (47 USC 151 et seq.)	1934	Regulates interstate and foreign telecommunications (amended 1996 and 2001)
Freedom of information	Freedom of Information Act (FOIA)	1966	Allows for the disclosure of previously unreleased information and documents controlled by the U.S. government
Privacy	Federal Privacy Act of 1974	1974	Governs federal agency use of personal information
Copyright	Copyright Act of 1976—Update to U.S. Copyright Law (17 USC)	1976	Protects intellectual property, including publications and software
Cryptography	Electronic Communications Privacy Act of 1986 (Update to 18 USC)	1986	Regulates interception and disclosure of electronic information; also referred to as the Federal Wiretapping Act
Access to stored communications	Unlawful Access to Stored Communications (18 USC 2701)	1986	Provides penalties for illegally accessing stored communications (such as e-mail and voicemail) stored by a service provider
Threats to computers	Computer Fraud and Abuse Act (also known as Fraud and Related Activity in Connection with Computers) (18 USC 1030)	1986	Defines and formalizes laws to counter threats from computer-related acts and offenses (amended 1996, 2001, and 2006)
Federal agency information security	Computer Security Act of 1987	1987	Requires all federal computer systems that contain classified information to have security plans in place, and requires periodic security training for all individuals who operate, design, or manage such systems

U.S. General Computer Crime Laws:

Computer Fraud and Abuse Act of 1986 (CFA Act)
- Cornerstone of federal laws and enforcement acts
- Addresses threats to computers

Communications Act of 1934
- Addresses Telecommunications

Computer Security Act of 1987
- Protect federal computer systems (federal agencies)
- Establish minimum acceptable security practices

International Laws and Legal Bodies:

European Council Cyper-Crime Convention
- 2001. Creates international task force
- Improve effectiveness of international investigations
- Emphasis on copyright infringement prosecution
- Lacks realistic provisions for enforcement

WTO Agreement on Intellectual Property Rights
- Intellectual property rules for multilateral trade system.

Digital Millennium Copyright Act**
- U.S. response to 1995 Directive 95/46/EC by E.U.
- U.K. Database Right

United Nations Charter
- Information Warfare provisions.

Ethics and Information Security:

Many Professional groups have explicit rules governing ethical behavior in the workplace. For example, doctors and lawyers who commit egregious violations of their professions' canons of conduct can be removed from practice. Unlike the medical and legal fields, however, the information technology field in general, and the information security field in particular, do not have a binding code of ethics. Instead, professional associations—such as the Association for Computing Machinery (ACM) and the Information Systems Security Association—and certification agencies—such as the International Information Systems Security Certification Consortium, Inc., or (ISC)2—work to establish the profession's ethical codes of conduct. While these professional organizations can prescribe ethical conduct, they do not always have the authority to banish violators from practicing their trade.

Week 03 – Topic 03

Code of Ethics

A number of professional organizations have established codes of conduct or codes of ethics that members are expected to follow. Codes of ethics can have a positive effect on people's judgment regarding computer use. Unfortunately, many employers do not encourage their employees to join these professional organizations. But employees who have earned some level of certification or professional accreditation can be deterred from ethical lapses by the threat of loss of accreditation or certification due to a violation of a code of conduct. Loss of certification or accreditation can dramatically reduce marketability and earning power. It is the responsibility of security professionals to act ethically and according to the policies and procedures of their employers, their professional organizations, and the laws of society. It is likewise the organization's responsibility to develop, disseminate, and enforce its policies.

The Ten Commandments of Computer Ethics

From The Computer Ethics Institute

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid.
7. Thou shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.

Week 03 – Topic 04

Professional Organizations

Association for Computing Machinery (ACM)

The Association of Computing Machinery (ACM) (www.acm.org) is a respected professional society that was established in 1947 as "the world's first educational and scientific computing society." It is one of the few organizations that strongly promotes education and provides discounts for student members. The ACM's code of ethics requires members to perform their duties in a manner befitting an ethical computing professional. The code contains specific references to protecting the confidentiality of information, causing no harm (with specific references to viruses), protecting the privacy of others, and respecting the intellectual property and copyrights of others. The ACM also publishes a wide variety of professional computing publications, including the highly regarded *Communications of the ACM*.

International Information Systems Security Certification Consortium $(ISC)^2$

The International Information Systems Security Certification Consortium, Inc. $(ISC)^2$ (www.isc2.org) is a nonprofit organization that focuses on the development and implementation of information security certifications and credentials. The $(ISC)^2$ manages a body of knowledge on information security and administers and evaluates examinations for information security certifications. The code of ethics put forth by $(ISC)^2$ is primarily designed for information security professionals who have earned an $(ISC)^2$ certification, and has four mandatory canons: "Protect society, the commonwealth, and the infrastructure; act honorably, honestly, justly, responsibly, and legally; provide diligent and competent service to principals; and advance and protect the profession." This code enables $(ISC)^2$ to promote reliance on the ethicality and trustworthiness of the information security professional as the guardian of information and systems.

System Administration, Networking, and Security Institute (SANS)

The System Administration, Networking, and Security Institute (SANS) (www.sans.org), which was founded in 1989, is a professional research and education cooperative organization with a current membership of more than 156,000 security professionals, auditors, system administrators, and network administrators. SANS offers a set of certifications called the Global Information Assurance Certification, or GIAC. All GIAC-certified professionals are required to acknowledge that certification and the privileges that come from it carry a corresponding obligation to uphold the GIAC Code of Ethics. Those certificate holders that do not conform to this code face punishment, and may lose GIAC certification.

Information Systems Audit and Control Association (ISACA)

The Information Systems Audit and Control Association (ISACA) (www.isaca.org) is a professional association that focuses on auditing, control, and security. The membership comprises both technical and managerial professionals. ISACA provides IT control practices and standards, and although it does not focus exclusively on information security, it does include many information security components within its areas of concentration. ISACA also has a code of ethics for its professionals, and it requires many of the same high standards for ethical performance as the other organizations and certifications.

Computer Security Institute (CSI)

Sponsors education and training for information security. The Computer Security Institute (CSI) was a professional membership organization serving practitioners of information, network, and computer-enabled physical security, from the level of system administrator to the chief information security officer. It was founded in 1974.

Information Systems Security Association (ISSA)

The Information Systems Security Association (ISSA) (www.issa.org) is a nonprofit society of information security professionals. As a professional association, its primary mission is to bring together qualified information security practitioners for information exchange and educational development. ISSA provides a number of scheduled conferences, meetings, publications, and information resources to promote information security awareness and education. ISSA also promotes a code of ethics, similar in content to those of $(ISC)^2$, ISACA, and the ACM, whose focus is "promoting management practices that will ensure the confidentiality, integrity, and availability of organizational information resources."

Other Security Organization

- Internet Society (ISOC)

Develop education, standards, policy, and education and training to promote the Internet.

- Internet Engineering Task Force (IETF)

Develops Internet's technical foundations.

- Computer Security Division (CSD) of National Institute for Standards and Technology (NIST)

Computer Security Resource Center (CSRC).

- Computer Emergency Response Team (CERT)

- CERT Coordination Center (CERT/CC)

Carnegie Mellon University Software Engineering Institute

- Computer Professionals for Social Responsibility (CPSR)

Promotes ethical and responsible development and use of computing

Week 04 – Topic 01

Why need Security?

- What threats can you think to your home?
- To your money (including bank accounts, checks, credit and debit cards)?
- To your home computer?

Home:	**Money (cash/credit):**	**Computer:**
– Burglary – Fire – Vandalism	– Theft. – Counterfeiting. – Signature forgery. – Identity theft.	– Viral/worm infection. – Adware/spyware. – Denial of service. – Data destruction. – Physical destruction – Use of computer for felonious purposes.

We need Security Because

- Information Security System copes with all these threats for an organization

Information Security Tasks

- Information security performs four important functions for an organization:
  1. Protects the organization's ability to function
  2. Enables the safe operation of applications implemented on the organization's IT systems
  3. Protects the data, the organization collects and uses
  4. Safeguards the technology assets in use at the organization

1. Protects the organization's ability to function

- Management is responsible
- Information security is
  - a management issue
  - a people issue
- Communities of interest must argue for information security in terms of impact and cost.

2. Enables the safe operation of applications

- Organizations must create integrated, efficient, and capable applications
- Organization need environments that safeguard applications
- Management must not abdicate to the IT department its responsibility to make choices and enforce decisions

3. Protects the Organizational data

- One of the most valuable assets is data.
- Without data, an organization loses its record of transactions and/or its ability to deliver value to its customers.
- An effective information security program is essential to protect the integrity and value of the organization's data.

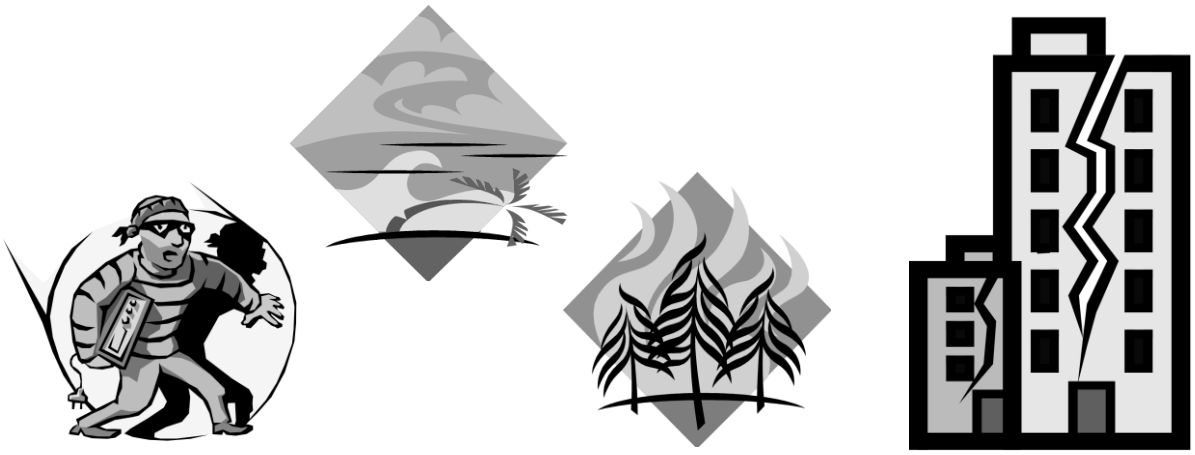
4. Safeguards the technology assets

- Organizations must have secure infrastructure services based on the size and scope of the enterprise.
- Additional security services may have to be provided.
- More robust solutions may be needed to replace security programs the organization has outgrown.

Week 04 – Topic 02

Threats

A threat is an object, person, or other entity that represents a constant danger to an asset.



Unlike any other information technology program, 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.

Types of Threats:

	Category of Threat	Examples
1.	Compromises to intellectual property	Piracy, copyright infringement
2.	Software attacks	Viruses, worms, macros, denial of service
3.	Deviations in quality of service	ISP, power, or WAN service issues from service providers
4.	Espionage or trespass	Unauthorized access and/or data collection
5.	Forces of nature	Fire, flood, earthquake, lightning
6.	Human error or failure	Accidents, employee mistakes
7.	Information extortion	Blackmail, information disclosure
8.	Missing, inadequate, or incomplete	Loss of access to information systems due to disk drive failure without proper backup and recovery plan organizational policy or planning in place
9.	Missing, inadequate, or incomplete controls	Network compromised because no firewall security controls
10.	Sabotage or vandalism	Destruction of systems or information
11.	Theft	Illegal confiscation of equipment or information
12.	Technical hardware failures or errors	Equipment failure
13.	Technical software failures or errors	Bugs, code problems, unknown loopholes
14.	Technological obsolescence	Antiquated or outdated technologies

Digital Threats

- Automation – Culprit can use automated procedures to infiltrate and capture data.
- Action at speed – The whole heist can take up to fraction of second to occur.
- Technique Propagation – The method of robbery can spread on the internet very fast.

Acts of 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. For example, a simple keyboarding error can cause worldwide Internet outages.

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—even, as Figure 2-1 suggests, relative to threats from outsiders. This is because employee mistakes can easily lead to the following: revelation of classified data, entry of erroneous data, accidental deletion or modification of data, storage of data in unprotected areas, and failure to protect information. Leaving classified information in unprotected areas, such as on a desktop, on a Web site, or even in the trash can, is as much a threat to the protection of the information as is the individual who seeks to exploit the information, because one person's carelessness can create a vulnerability and thus an opportunity for an attacker. However, if someone damages or destroys data on purpose, the act belongs to a different threat category.

FIGURE 2-1 Acts of Human Error or Failure

Much human error or failure can be prevented with training and ongoing awareness activities, but also with controls, ranging from simple procedures, such as requiring the user to type a critical command twice, to more complex procedures, such as the verification of commands by a second party. An example of the latter is the performance of key recovery actions in PKI systems. Many military applications have robust, dual-approval controls built in. Some systems that have a high potential for data loss or system outages use expert systems to monitor human actions and request confirmation of critical inputs.

Deviations in Quality of Service by Service Providers

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.

- Three sets of service issues that dramatically affect the availability of information and systems are
  - Internet service
  - Communications
  - Power irregularities

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. When an organization places its Web servers in the care of a Web hosting provider, that provider assumes responsibility for all Internet services as well as for the hardware and operating system software used to operate the Web site. These Web hosting services are usually arranged with an agreement providing minimum service levels known as a Service Level Agreement (SLA). When a service provider fails to meet the SLA, the provider may accrue fines to cover losses incurred by the client, but these payments seldom cover the losses generated by the outage.

Communications and Other Services

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. Air conditioning systems help keep a modern facility operating. If a wastewater system fails, an organization might be prevented from allowing employees into the building.

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.

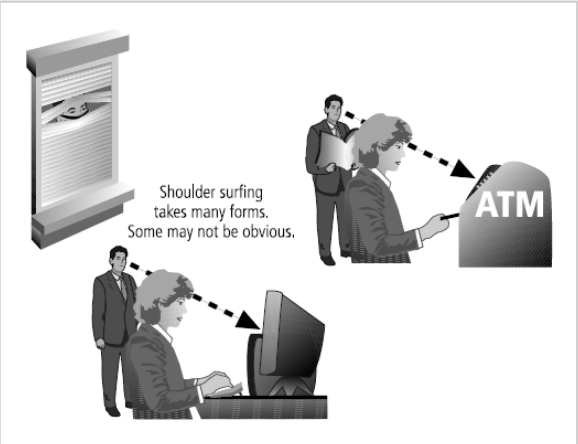
- Voltage levels can increase, decrease, or cease:
  - Spike – momentary increase
  - Surge – prolonged increase
  - Sag – momentary low voltage
  - Brownout – prolonged drop
  - Fault – momentary loss of power
  - Blackout – prolonged loss

Because sensitive electronic equipment—especially networking equipment, computers, and computer-based systems—are vulnerable to fluctuations, controls should be applied to manage power quality. With small computers and network systems, quality power-conditioning options such as surge suppressors can smooth out spikes. The more expensive uninterruptible power supply (UPS) can protect against spikes and surges as well as against sags and even blackouts of limited duration.

Week 04 – Topic 03

Espionage/Trespass

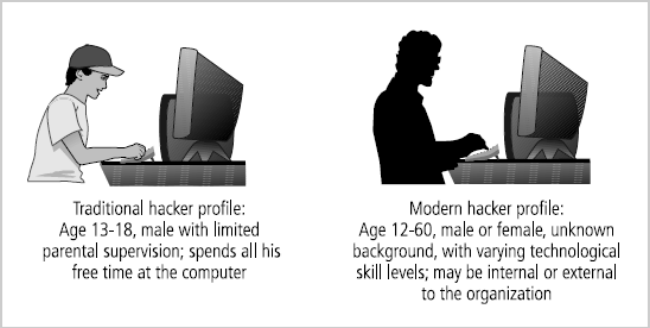
Espionage or trespass is a well-known and broad category of electronic and human activities that can breach the confidentiality of information. When an unauthorized individual gains access to the information an organization is trying to protect, that act is categorized as espionage or trespass. Attackers 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. One example, called shoulder surfing, is pictured in Figure.



This technique is used in public or semipublic settings when individuals gather information they are not authorized to have by looking over another individual's shoulder or viewing the information from a distance. Instances of shoulder surfing occur at computer terminals, desks, ATM machines, on the bus or subway where people use smartphones and tablet PCs, or other places where a person is accessing confidential information. There is unwritten etiquette among professionals who address information security in the workplace. When someone can see another person entering personal or private information into a system, the first person should look away as the information is entered. Failure to do so constitutes not only a breach of etiquette, but an affront to privacy as well as a threat to the security of confidential information.

Acts of trespass can lead to unauthorized real or virtual actions that enable information gatherers to enter premises or systems they have not been authorized to enter. Controls sometimes mark the boundaries of an organization's virtual territory. These boundaries give notice to trespassers that they are encroaching on the organization's cyberspace. Sound principles of authentication and authorization can help organizations protect valuable information and systems. These control methods and technologies employ multiple layers or factors to protect against unauthorized access.

The classic perpetrator of espionage or trespass is the hacker. Hackers are "people who use and create computer software [to] gain access to information illegally." Hackers are frequently glamorized in fictional accounts as people who stealthily manipulate a maze of computer networks, systems, and data to find the information that solves the mystery or saves the day. Television and motion pictures are inundated with images of hackers as heroes or heroines. However, the true life of the hacker is far more mundane. In the real world, a hacker frequently spends long hours examining the types and structures of the targeted systems and uses skill, guile, or fraud to attempt to bypass the controls placed around information that is the property of someone else.



There are generally two skill levels among hackers. The first is the expert hacker, or elite hacker, who develops software scripts and program exploits used by those in the second category, the novice or unskilled hacker. The expert hacker is usually a master of several programming languages, networking protocols, and operating systems and also exhibits a mastery of the technical environment of the chosen targeted system. Expert hackers are extremely talented individuals who usually devote lots of time and energy to attempting to break into other people's information systems. Once an expert hacker chooses a target system, the likelihood that he or she will successfully enter the system is high. Fortunately for the many poorly protected organizations in the world, there are substantially fewer expert hackers than novice hackers.

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.

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. Compared to Web site defacement, vandalism within a network is more malicious in intent and less public. Today, security experts are noticing a rise in another form of online vandalism, hacktivist or cyber-activist operations, which interfere with or disrupt systems to protest the operations, policies, or actions of an organization or government agency. A much more sinister form of hacking is cyber-terrorism. Cyber-terrorists hack systems to conduct terrorist activities via network or Internet pathways.

Deliberate Acts of 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.

Week 05 – Topic 01

Software Attacks

- Introduction
- Types of Software Attacks
- Software Attacks

Attack

- An attack is any action that violates security.

- An attack has an implicit concept of "intent".
  - Router misconfiguration or server crash can also cause loss of availability, but they are not attacks.

Some Terminologies:

Exploit: An exploit is a technique to compromise a system.

Vulnerability: A vulnerability is an identified weakness of a controlled system whose controls are not present or are no longer effective.

Security attack: Any actions that compromises the security of information owned by an organization (or a person).

Security mechanism: A mechanism that is designed to detect, prevent, or recover from a security attack.

Security Policy: a statement of what is, and is not allowed.

Security Controls: Security controls are safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets.

Security service: A service that enhances the security of the data processing systems and the information transfers of an organization. The services make use of one or more security mechanisms to provide the service.

Technical Definition of attack:
An attack is the deliberate act that exploits vulnerability.

Threat *vs* Attack
Threat
A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.
Attack
An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

Week 05 – Topic 02

Types of Software Attacks

There are two types of Software attacks:

1. Active Attacks

Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories:

a) Masquerade.
b) Replay.
c) Modification of messages.
d) Denial of service.

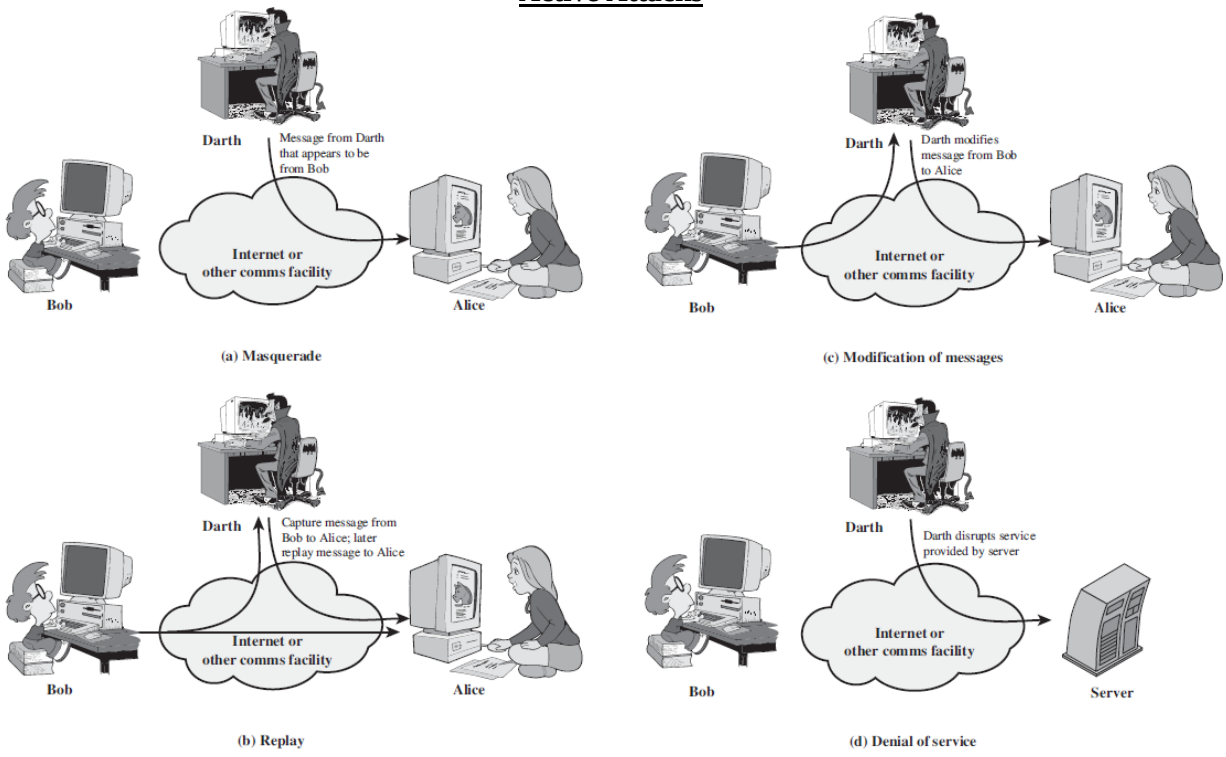
A **masquerade** takes place when one entity pretends to be a different entity. A masquerade attack usually includes one of the other forms of active attack. For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.

Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

Modification of messages simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect. For example, a message meaning "Allow John Smith to read confidential file accounts" is modified to mean "Allow Fred Brown to read confidential file accounts."

The denial of service prevents or inhibits the normal use or management of communications facilities. This attack may have a specific target; for example, an entity may suppress all messages directed to a particular destination (e.g., the security audit service).Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance.

Active Attacks



2. Passive attacks

Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted.

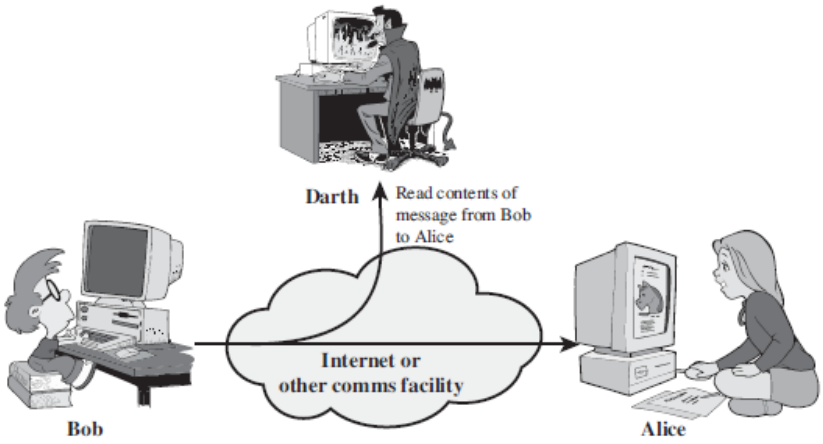
Two types of passive attacks are:

a) Release of message contents.
b) Traffic analysis.

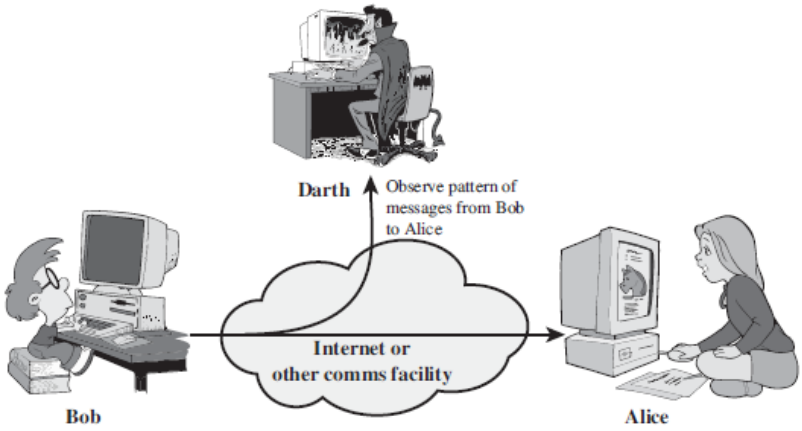
The **release of message contents** is easily understood. A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.

A second type of passive attack, **traffic analysis**, is subtler. Suppose that we had a way of masking the contents of messages or other information traffic so that opponents, even if they captured the message, could not extract the information from the message. The common technique for masking contents is encryption. If we had encryption protection in place, an opponent might still be able to observe the pattern of these messages. The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.

Passive Attacks



(a) Release of message contents



(b) Traffic analysis

How to deal with Active Attack?

It is quite difficult to prevent active attacks absolutely because of the wide variety of potential physical, software, and network vulnerabilities. Instead, the goal is to detect active attacks and to recover from any disruption or delays caused by them. If the detection has a deterrent effect, it may also contribute to prevention.

How to deal with Passive Attack?

Passive attacks are very difficult to detect, because they do not involve any alteration of the data. Typically, the message traffic is sent and received in an apparently normal fashion, and neither the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern. However, it is feasible to prevent the success of these attacks, usually by means of encryption. Thus, the emphasis in dealing with passive attacks is on prevention rather than detection.

Software 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. 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 multi-vector, worm. These attack programs use up to six known attack vectors to exploit a variety of vulnerabilities in commonly found information system devices.

1) IP scan and attack
2) Web browsing
3) Virus
4) Unprotected shares
5) Mass mail
6) Simple Network Management Protocol (SNMP)

Perhaps the best illustration of such an attack remains the outbreak of Nimda in September 2001, which used five of the six vectors to spread itself with startling speed. TruSecure Corporation, an industry source for information security statistics and solutions, reports that Nimda spread to span the Internet address space of 14 countries in less than 25 minutes.

Other forms of malware include covert software applications:

i. Bots,
ii. Spyware
iii. Adware

These are designed to work out of sight of users or via an apparently innocuous user action.

A **bot** (an abbreviation of robot) is "an automated software program that executes certain commands when it receives a specific input. Bots are often the technology used to implement Trojan horses, logic bombs, back doors, and spyware."

Spyware is "any technology that aids in gathering information about a person or organization without their knowledge. Spyware is placed on a computer to secretly gather information about the user and report it. The various types of spyware include

a) A Web bug, a tiny graphic on a Web site that is referenced within the Hypertext Markup Language (HTML) content of a Web page ore-mail to collect information about the user viewing the HTML content;
b) A tracking cookie, which is placed on the user's computer to track the user's activity on different Web sites and create a detailed profile of the user's behavior.

Adware is "any software program intended for marketing purposes such as that used to deliver and display advertising banners or popups to the user's screen or tracking the user's online usage or purchasing activity." Each of these hidden code components can be used to collect information from or about the user which could then be used in a social engineering or identity theft attack.

2. IP scan and attack:
The infected system scans a random or local range of IP addresses and targets any of several vulnerabilities known to hackers or left over from previous exploits such as Code Red, Back Orifice, or PoizonBox.

3. Web browsing:
If the infected system has write access to any Web pages, it makes all Web content files (.html, .asp, .cgi, and others) infectious, so that users who browse to those pages become infected.

4. Unprotected shares:
Using vulnerabilities in file systems and the way many organizations configure them, the infected machine copies the viral component to all locations it can reach.

5. Mass mail:
By sending e-mail infections to addresses found in the address book, the infected machine infects many users, whose mail-reading programs also automatically run the program and infect other systems.

6. Simple Network Management Protocol (SNMP):
By using the widely known and common passwords that were employed in early versions of this protocol (which is used for remote management of network and computer devices), the attacking program can gain control of the device. Most vendors have closed these vulnerabilities with software upgrades.

7. 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.

8. 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. 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.

9. 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.

10. 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.

11. 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.

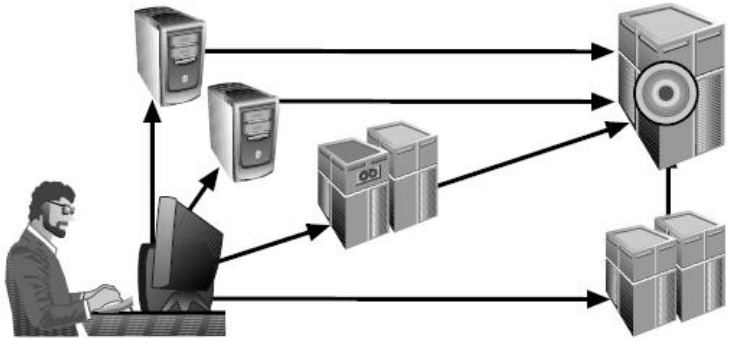
Week 05 – Topic 03

12. Denial-of-service (DoS):

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.

13. Distributed Denial-of-service (DDoS):

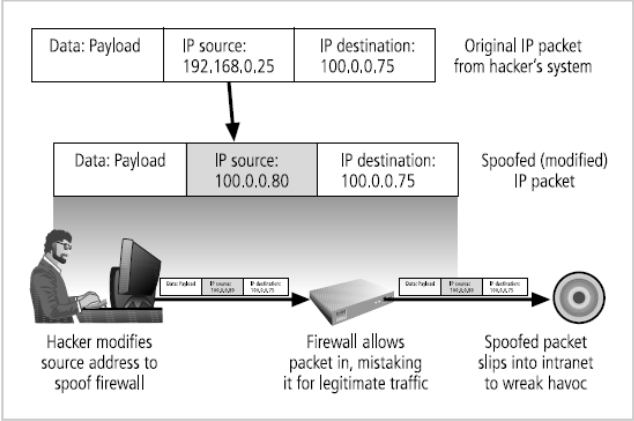
A distributed denial of- service (DDoS) is an attack in which a coordinated stream of requests is launched against a target from many locations at the same time. Most DDoS attacks are preceded by a preparation phase in which many systems, perhaps thousands, are compromised. The compromised machines are turned into zombies, machines that are directed remotely (usually by a transmitted command) by the attacker to participate in the attack.



Any system connected to the Internet and providing TCP-based network services (such as a Web server, FTP server, or mail server) is vulnerable to DoS attacks. DoS attacks can also be launched against routers or other network server systems if these hosts enable (or turn on) other TCP services (e.g., echo).

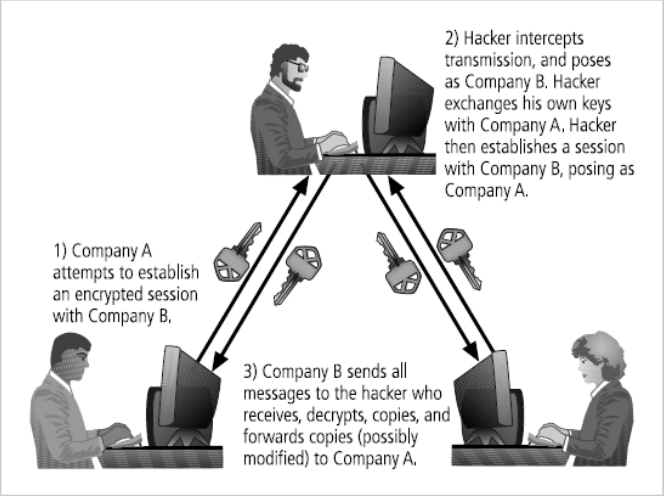
14. Spoofing:

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.



15. 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. Figure Illustrates these attacks by showing how a hacker uses public and private encryption keys to intercept messages.



16. 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. 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.

17. 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 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.

18. 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.

19. 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. For instance, anyone can check a company's Web site, or even call the main switchboard to get the name of the Chief Information Officer (CIO); an attacker may then obtain even more information by calling others in the company and asserting his or her (false) authority by mentioning the CIO's name. Social engineering attacks may involve individuals posing as new employees or as current employees requesting assistance to prevent getting fired. Sometimes attackers threaten, persuade, or beg to sway the target.

20. Buffer Overflow:

Buffers are used to manage mismatches in the processing rates between two entities involved in a communication process. A 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.

21. Ping of Death Attacks:

It is a type of Denial of service (DoS) attack. In it Attacker creates an ICMP packet that is larger than the maximum allowed 65,535 bytes. Destination user machine cannot handle the reassembled oversized packet, thereby causing the system to crash or freeze.

22. 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.

Week 06 – Topic 01

Security Policy

Security analysts organize the needs of a site in order to define a security policy. From this policy, analysts develop and implement mechanisms for enforcing the policy. The mechanisms may be procedural, technical, or physical. A security policy defines "secure" for a system or a set of systems. Security policies can be informal or highly mathematical in nature. After defining a security policy precisely, we expand on the nature of "trust" and its relationship to security policies.

Introduction

- Primary mission of information security is to ensure that systems and contents stay the same.
- A security policy sets the context in which we can define a secure system.
- Security policy defines what it means for a system to be secure.

Definition 1: A *security policy* is a statement that partitions the states of the system into a set of *authorized*, or *secure*, states and a set of *unauthorized*, or *non-secure*, states. A security policy sets the context in which we can de□ne a secure system. What is secure under one policy may not be secure under a different policy.

Definition 2: A *secure* system is a system that starts in an authorized state and cannot enter an unauthorized state.

Definition 3: A breach of security occurs when a system enters an unauthorized state.

A security policy considers all relevant aspects of confidentiality, integrity, and availability.

With respect to **confidentiality**, it identifies those states in which information leaks to those not authorized to receive it. This includes the leakage of rights and the illicit transmission of information without leakage of rights, called information flow. Also, the policy must handle changes of authorization, so it includes a temporal element. For example, a contractor working for a company may be authorized to access proprietary information during the lifetime of a nondisclosure agreement, but when that nondisclosure agreement expires, the contractor can no longer access that information. This aspect of the security policy is often called a confidentiality policy.

With respect to **integrity**, a security policy identifies authorized ways in which information may be altered and entities authorized to alter it. Authorization may derive from a variety of relationships, and external influences may constrain it; for example, in many transactions, a principle called separation of duties forbids an entity from completing the transaction on its own. Those parts of the security policy that describe the conditions and manner in which data can be altered are called the integrity policy.

With respect to **availability**, a security policy describes what services must be provided. It may present parameters within which the services will be accessible— for example, that a browser may download web pages but not Java applets. It may require a level of service—for example, that a server will provide authentication data within 1 minute of the request being made. This relates directly to issues of quality of service.

Policy Model

Gives abstract description of a policy or class of policies. A security model is a model that represents a particular policy or set of policies. It focuses on points of interest in policies.

For example:

- It focuses on "Security levels" in multilevel security models.
- It focuses on "Separation of duty" in Clark-Wilson model.
- It focuses on "Conflict of interest" in Chinese Wall model.

The statement of a security policy may formally state the desired properties of the system. If the system is to be provably secure, the formal statement will allow the designers and implementers to prove that those desired properties hold. If a formal proof is unnecessary or infeasible, analysts can test that the desired properties hold for some set of inputs.

In practice, a less formal type of security policy defines the set of authorized states. Typically, the security policy assumes that the reader understands the context in which the policy is issued—in particular, the laws, organizational policies, and other environmental factors. The security policy then describes conduct, actions, and authorizations defining "authorized users" and "authorized use."

EXAMPLE:

A university disallows cheating, which is defined to include copying another student's homework assignment (with or without permission). A computer science class requires the students to do their homework on the department's computer. One student notices that a second student has not read-protected the file containing her homework and copies it.

Has either student (or have both students) breached security?

The second student has not, despite her failure to protect her homework. The security policy requires no action to prevent files from being read. Although she may have been too trusting, the policy does not ban this; hence, the second student has not breached security.

The first student has breached security. The security policy disallows the copying of homework, and the student has done exactly that. Whether the security policy specifically states that "files containing homework shall not be copied" or simply says that "users are bound by the rules of the university" is irrelevant; in the latter case, one of those rules bans cheating. If the security policy is silent on such matters, the most reasonable interpretation is that the policy disallows actions that the university disallows, because the computer science department is part of the university.

Policy vs. Mechanism

The reply that the first user could copy the files, and therefore the action is allowed, confuses mechanism with policy. The distinction is sharp:

Definition: A *security policy* is a statement that partitions the states of the system into a set of *authorized*, or *secure*, states and a set of *unauthorized*, or *non-secure*, states.

Definition: A *security mechanism* is an entity or procedure that enforces some part of the security policy.

EXAMPLE:
In the preceding example, the policy is the statement that no student may copy another student's homework. One mechanism is the file access controls; if the second student had set permissions to prevent the first student from reading the file containing her homework, the first student could not have copied that file.

Security policies are often implicit rather than explicit. This causes confusion, especially when the policy is defined in terms of the mechanisms. This definition may be ambiguous—for example, if some mechanisms prevent a specific action and others allow it. Such policies lead to confusion, and sites should avoid them.

Policy Language

A policy language is a language for representing a security policy. *High-level policy* languages express policy constraints on entities using abstractions. *Low-level policy* languages express constraints in terms of input or invocation options to programs existing on the systems. So Policy Language expresses security policies in a precise way.

High Level Policy Language

A policy is independent of the mechanisms. It describes constraints placed on entities and actions in a system. A high-level policy language is an unambiguous expression of policy.
Example:
A policy restricts the actions of Java programs that are downloaded and executed under control of web browser.

Low Level Policy Language

A low-level policy language is simply a set of inputs or arguments to commands that set, or check, constraints on a system.
EXAMPLE:
The UNIX-based windowing system X11 provides a language for controlling access to the console (on which X11 displays its images). The language consists of a command, xhost, and a syntax for instructing the command to allow access based on host name (IP address).
For example,
xhost +groucho –chico
This sets the system so that connections from the host groucho are allowed but connections from chico are not.

Week 06 – Topic 02

Types of Security Policies

Each site has its own requirements for the levels of confidentiality, integrity, and availability, and the site policy states these needs for that particular site.

Military (governmental) security policy:

A military security policy (also called a governmental security policy) is a security policy developed primarily to provide confidentiality.

The name comes from the military's need to keep some information secret, such as the date that a troop ship will sail. Although integrity and availability are important, organizations using this class of policies can overcome the loss of either—for example, by using orders not sent through a computer network. But the compromise of confidentiality would be catastrophic, because an opponent would be able to plan countermeasures (and the organization may not know of the compromise).

Commercial security policy:

A commercial security policy is a security policy developed primarily to provide integrity.

The name comes from the need of commercial firms to prevent tampering with their data, because they could not survive such compromises. For example, if the confidentiality of a bank's computer is compromised, a customer's account balance may be revealed. This would certainly embarrass the bank and possibly cause the customer to take her business elsewhere. But the loss to the bank's "bottom line" would be minor. However, if the integrity of the computer holding the accounts were compromised, the balances in the customers' accounts could be altered, with financially ruinous effects.

Also for example, a company is launching a new revolutionary health product so its formula is very secretive and its integrity is very important.

Confidentiality policy:

A confidentiality policy is a security policy dealing only with confidentiality.

Example:

- Final Paper of university cannot be disclosed. As it is confidential information.
- Another example is, if the confidentiality of a bank's computer is compromised, a customer's account balance may be revealed.

Integrity policy:

An integrity policy is a security policy dealing only with integrity.

Example:

When a customer moves money from one account to another, the bank uses a well-formed transaction. This transaction has two distinct parts:

Money is first debited to the original account and then credited to the second account.

Unless both parts of the transaction are completed, the customer will lose the money. With a well-formed transaction, if the transaction is interrupted, the state of the database is still consistent—either as it was before the transaction began or as it would have been when the transaction ended. Hence, part of the bank's security policy is that all transactions must be well-formed.

Both confidentiality policies and military policies deal with confidentiality. However, a confidentiality policy does not deal with integrity at all, whereas a military policy may. A similar distinction holds for integrity policies and commercial policies.

Types of Access Control

Discretionary access control (DAC)

If an individual user can set an access control mechanism to allow or deny access to an object, that mechanism is a *discretionary access control (DAC)*, also called an *identity-based access control (IBAC).*

Discretionary access controls base access rights on the identity of the subject and the identity of the object involved. Identity is the key; the owner of the object constrains who can access it by allowing only particular subjects to have access. The owner states the constraint in terms of the identity of the subject, or the owner of the object.

EXAMPLE:

Suppose a child keeps a diary. The child controls access to the diary, because she can allow someone to read it (grant read access) or not allow someone to read it (deny read access). The child allows her mother to read it, but no one else. This is a discretionary access control because access to the diary is based on the identity of the subject (mom) requesting read access to the object (the diary).

Mandatory Access Control (MAC)

The second type of access control is based on authorization, and identity is irrelevant. When a system mechanism controls access to an object and an individual user cannot alter that access, the control is a *mandatory access control (MAC)*, occasionally called a *rule-based access control*.

The operating system enforces mandatory access controls. Neither the subject nor the owner of the object can determine whether access is granted. Typically, the system mechanism will check attributes associated with both the subject and the object to determine whether the subject should be allowed to access the object. Rules describe the conditions under which access is allowed.

EXAMPLE:

The law allows a court to access driving records without an owner's permission. This is a mandatory control, because the owner of the record has no control over the court's access to the information.

Originator Controlled Access Control (ORCON)

An *originator controlled access control* (ORCON or ORGCON) bases access on the creator of an object (or the information it contains).

The goal of this control is to allow the originator of the file (or of the information it contains) to control the dissemination of the information. The owner of the file has no control over who may access the file.

EXAMPLE:

Bit Twiddlers, Inc., a company famous for its embedded systems, contracts with Microhackers Ltd., a company equally famous for its microcoding abilities. The contract requires Microhackers to develop a new microcode language for a particular processor designed to be used in high-performance embedded systems. Bit Twiddlers gives Microhackers a copy of its specifications for the processor. The terms of the contract require Microhackers to obtain permission before it gives any information about the processor to its subcontractors. This is an originator controlled access mechanism because, even though Microhackers owns

the file containing the specifications, it may not allow anyone to access that information unless the creator of that information, Bit Twiddlers, gives permission.

Role of Trust

The role of trust is crucial to understanding the nature of computer security. Theories and mechanisms for analyzing and enhancing computer security are presented, but any theories or mechanisms rest on certain assumptions. When someone understands the assumptions her security policies, mechanisms, and procedures rest on, she will have a very good understanding of how effective those policies, mechanisms, and procedures are.

A system administrator receives a security patch for her computer's operating system. She installs it. Has she improved the security of her system? She has indeed, given the correctness of certain assumptions:

- *She is assuming that the patch came from the vendor and was not tampered with in transit*, rather than from an attacker trying to trick her into installing a bogus patch that would actually open security holes.
- *She is assuming that the vendor tested the patch thoroughly*. Vendors are often under considerable pressure to issue patches quickly and sometimes test them only against a particular attack. The vulnerability may be deeper, however, and other attacks may succeed.
- *She is assuming that the vendor's test environment corresponds to her environment.* Otherwise, the patch may not work as expected. As an example, a vendor's patch once enabled the host's personal firewall, causing it to block incoming connections by default. This prevented many programs from functioning. The host had to be reconfigured to allow the programs to continue to function. This assumption also covers possible conflicts between different patches, such as patches from different vendors of software that the system is using.
- *She is assuming that the patch is installed correctly.* Some patches are simple to install, because they are simply executable files. Others are complex, requiring the system administrator to reconfigure network oriented properties, add a user, modify the contents of a registry, give rights to some set of users, and then reboot the system. An error in any of these steps could prevent the patch from correcting the problems, as could an inconsistency between the environments in which the patch was developed and in which the patch is applied. Furthermore, the patch may claim to require specific privileges, when in reality the privileges are unnecessary and in fact dangerous.

Week 06 – Topic 03

Confidentiality

- Data Confidentiality is whether the information stored on a system is protected against unintended or unauthorized access.
- Since systems are sometimes used to manage sensitive information, Data Confidentiality is often a measure of the ability of the system to protect its data.
- Accordingly, this is an integral component of Security.

Confidentiality Policy

- Also known as *information flow policy*.
- Goal: To prevent the unauthorized disclosure of information.
  - Deals with the flow of information.
- It is Highly developed in Military/Government areas.
- Multi-level security models are best-known examples of confidentiality policy.
  - Bell-LaPadula Model basis for many, or most, of these security models.

Integrity

- The ability to ensure that data is an accurate and unchanged representation of the original secure information.
- Requirements for integrity are very different than confidentiality policies.
- Integrity policies deal with trust. As trust is hard to quantify, so these policies are hard to evaluate completely.

Integrity Policies

- Biba's Integrity Policy Model
- LOCUS Integrity Policy Model
- Low Water Mark Policy
- Ring policy
- Integrity Matrix Model

Hybrid Model

- There are hybrid models which achieve both confidentiality and integrity.

Hybrid Model Policies

- Chinese Wall Model
- Role-Based Access Control (RBAC)
- Originator Controlled Access Control ORCON
- Clinical Information Systems Security Policy

Developing Information Systems Security Policies

- **Design**
  - Policy is designed. What will this policy deal with?

- **Implement**
  - How many levels are involved in the policy? Where is it going to effect?
- **Publish**
  - Policy document is published.
- **Enforce**
  - It is enforced throughout the organization.
- **Monitor compliance**
  - You check whether it is strictly followed or not.
- **Evaluate**
  - What is its effect? How is it working?
- **Review**
  - Is our policy still up to date or has is become vulnerable.
- **Amend and update**
  - What are the updates? Policy has to be updated.

Stakeholders

These are the persons who are directly or indirectly effected by the policy or are concerned with the policy.

- **Security experts**
  - They are the one who design, review and update the policy.
- **System / network administrators**
  - They implement security controls and provide guidelines.
- **Management**
  - They set security goals
  - They also provide resources
- **Users**
  - They follow security procedures
- **Auditors**
  - They are the one who monitors and check the compliance level.

Week 07 – Topic 01

Risk:

A risk is a potential problem – *it might happen and it might not.*

Conceptual definition of risk:

- Risk concerns future happenings
- Risk involves change in mind, opinion, actions, places, etc.
- Risk involves choice and the uncertainty that choice entails.

Two characteristics of risk:

1. **Uncertainty** – the risk may or may not happen, that is, there are no 100% risks (those, instead, are called constraints)
2. **Loss** – the risk becomes a reality and unwanted consequences or losses occur

Risk Categorization (Approach 1)

Project risks

- They threaten the project plan.
- If they become real, it is likely that the project schedule will slip and that costs will increase.

Technical risks

- They threaten the quality and timeliness of the software to be produced.
- If they become real, implementation may become difficult or impossible.

Business risks

- They threaten the viability of the software to be built.
- If they become real, they jeopardize the project or the product.

Risk Categorization (Approach 2)

Known risks

Those risks that can be uncovered after careful evaluation of the project plan, the business and technical environment in which the project is being developed, and other reliable information sources. (e.g., unrealistic delivery date)

Predictable risks

Those risks that are extrapolated from past project experience. (e.g., past turnover)

Unpredictable risks

Those risks that can and do occur, but are extremely difficult to identify in advance. (e.g., Developer leaves)

Risk Strategies

Reactive risk strategies

"Don't worry, I'll think of something."

- The majority of software teams and managers rely on this approach.
- Nothing is done about risks until something goes wrong.
- Crisis management is the choice of management techniques.

Proactive risk strategies

- Steps for risk management are followed.
- Primary objective is to avoid risk and to have a contingency plan in place to handle unavoidable risks in a controlled and effective manner.

Week 07 – Topic 02

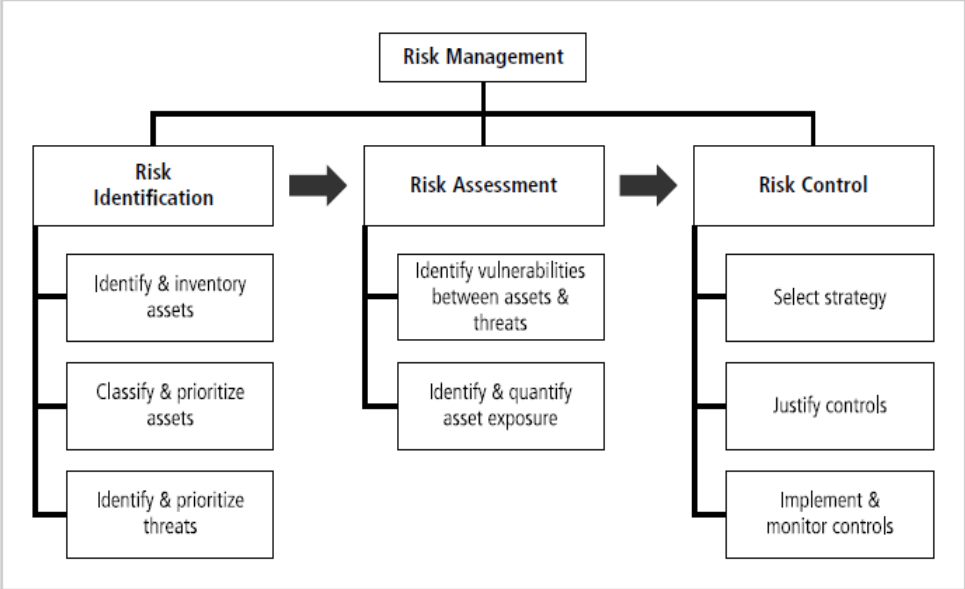
Risk Management:

Risk management is the process of identifying risk, as represented by vulnerabilities, to an organization's information assets and infrastructure, and taking steps to reduce this risk to an acceptable level. Each of the three elements in the C.I.A. triangle is an essential part of every IT organization's ability to sustain long-term competitiveness. When an organization depends on IT-based systems to remain viable, information security and the discipline of risk management must become an integral part of the economic basis for making business decisions. These decisions are based on trade-offs between the costs of applying information systems controls and the benefits realized from the operation of secured, available systems.

Risk management involves three major undertakings:

1. ***Risk identification*** is the examination and documentation of the security posture of an organization's information technology and the risks it faces.
2. ***Risk assessment*** is the determination of the extent to which the organization's information assets are exposed or at risk.
3. ***Risk control*** is the application of controls to reduce the risks to an organization's data and information systems.

Components of Risk Management



Risk Management is identifying, evaluating, and mitigating risk to an organization.

Steps:

1. *Identify* possible risks; recognize what can go wrong.
2. *Analyze* each risk to estimate the probability that it will occur and the impact (i.e., damage) that it will do if it does occur.
3. *Rank* the risks by probability and impact.
   - Impact may be negligible, marginal, critical, and catastrophic.
4. *Develop* a contingency plan to manage those risks having high probability and high impact.

An observation made over 2,400 years ago by Chinese General Sun Tzu Wu has direct relevance to information security today.

If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.

Know Yourself

First, you must identify, examine, and understand the information and systems currently in place within your organization. This is self-evident. To protect assets, which are defined here as information and the systems that use, store, and transmit information, you must know what they are, how they add value to the organization, and to which vulnerabilities they are susceptible. Once you know what you have, you can identify what you are already doing to protect it. Just because a control is in place does not necessarily mean that the asset is protected. Frequently, organizations implement control mechanisms but then neglect the necessary periodic review, revision, and maintenance. The policies, education and training programs, and technologies that protect information must be carefully maintained and administered to ensure that they remain effective.

Know the Enemy

Having identified your organization's assets and weaknesses, you move on to Sun Tzu's second step: Know the enemy. This means identifying, examining, and understanding the threats facing the organization. You must determine which threat aspects most directly affect the security of the organization and its information assets, and then use this information to create a list of threats, each one ranked according to the importance of the information assets that it threatens.

The Roles of the Communities of Interest

Each community of interest has a role to play in managing the risks that an organization encounters. Because the members of the information security community best understand the threats and attacks that introduce risk into the organization, they often take a leadership role in addressing risk. Management and users, when properly trained and kept aware of the threats the organization faces, play a part in the early detection and response process.

- *Management* must also ensure that sufficient resources (money and personnel) are allocated to the information security and information technology groups to meet the security needs of the organization.
- *Users* work with the systems and the data and are therefore well positioned to understand the value these information assets offer the organization and which assets among the many in use are the most valuable.
- *The information technology community* of interest must build secure systems and operate them safely. For example, IT operations ensure good backups to control the risk from hard drive failures.

The IT community can provide both valuation and threat perspectives to management during the risk management process.

All of the communities of interest must work together to address all levels of risk, which range from disasters that can devastate the whole organization to the smallest employee mistakes.

The three communities of interest are also responsible for the following:

- Evaluating the risk controls
- Determining which control options are cost effective for the organization
- Acquiring or installing the needed controls
- Ensuring that the controls remain effective

It is essential that all three communities of interest conduct periodic management reviews. The first focus of management review is asset inventory. On a regular basis, management must verify the completeness and accuracy of the asset inventory. In addition, organizations must review and verify the threats to and vulnerabilities in the asset inventory, as well as the current controls and mitigation strategies. They must also review the cost effectiveness of each control and revisit the decisions on deployment of controls. Furthermore, managers at all levels must regularly verify the ongoing effectiveness of every control deployed.

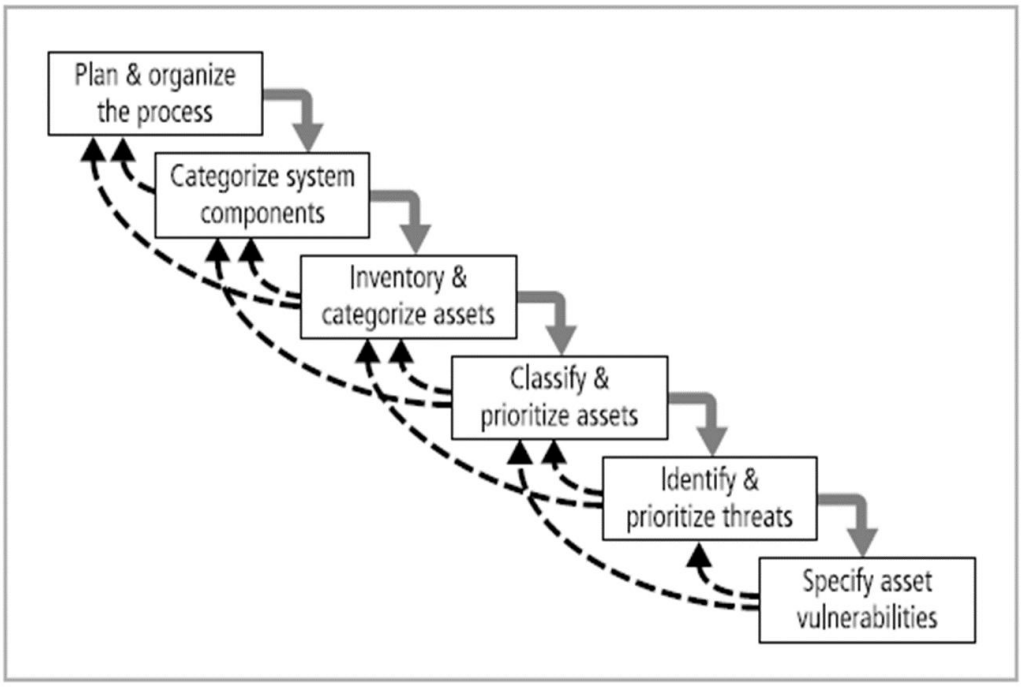
For example:
A sales manager might assess control procedures by walking through the office before the workday starts, picking up all the papers from every desk in the sales department. When the workers show up, the manager could inform them that a fire had been simulated and all of their papers destroyed, and that each worker must now follow the disaster recovery procedures to assess the effectiveness of the procedures and suggest corrections.

Week 07 – Topic 03

Risk Identification

A risk management strategy requires that information security professionals know their organizations' information assets—that is, identify, classify, and prioritize them. Once the organizational assets have been identified, a threat assessment process identifies and quantifies the risks facing each asset.

The components of risk identification



Plan and Organize the Process

Just as with any major information security undertaking, the first step in the Risk Identification process is to follow your project management principles. You begin by organizing a team, typically consisting of representatives of all affected groups. With risk identification, since risk can exist everywhere in the organization, representatives will come from every department from users, to managers, to IT and InfoSec groups. The process must then be planned out, with periodic deliverables, reviews, and presentations to management. Once the project is ready to begin, a meeting begins, tasks are laid out, assignments made, and timetables discussed. Only then is the organization ready to actually begin the next step—identifying and categorizing assets.

Asset Identification and Inventory

This iterative process begins with the enumeration of assets, including all of the elements of an organization's system, such as people, procedures, data and information, software, hardware, and networking elements. Then, you classify and categorize the assets, adding details as you dig deeper into the analysis. The objective of this process is to establish the relative priority of the assets to the success of the organization.

Categorizing the Components of an Information System

Traditional System Components	SesSDLC Components	Risk Management System Components
People	Employees	Trusted employees Other staff
	Nonemployees	People at trusted organizations Strangers
Procedures	Procedures	IT and business standard procedures IT and business sensitive procedures
Data	Information	Transmission Processing Storage
Software	Software	Applications Operating systems Security components
Hardware	System devices and peripherals	Systems and peripherals Security devices
	Networking components	Intranet components Internet or DMZ components

Identifying and categorizing assets

This iterative process begins with the enumeration of assets, including all of the elements of an organization's system, such as people, procedures, data and information, software, hardware, and networking elements. Then, you classify and categorize the assets, adding details as you dig deeper into the analysis. The objective of this process is to establish the relative priority of the assets to the success of the organization.

- People, Procedures, and Data Asset Identification:
  Identifying human resources, documentation, and data assets is more difficult than identifying hardware and software assets. People with knowledge, experience, and judgment should be assigned the task. As the people, procedures, and data assets are identified, they should be recorded using a reliable data handling process. Whatever record keeping mechanism you use, be sure it has the flexibility to allow the specification of attributes particular to the type of asset. Some attributes are unique to a class of elements.

- Hardware, Software, and Network Asset Identification:
  Which attributes of hardware, software, and network assets should be tracked? It depends on the needs of the organization and its risk management efforts, as well as the preferences and needs of the information security and information technology communities.

- Automated Asset Inventory Tools:
  Automated tools can sometimes identify the system elements that make up hardware, software, and network components. For example, many organizations use automated asset inventory systems. The inventory listing is usually available in a database or can be exported to a database for custom information on security assets. Once stored, the inventory listing must be kept current, often by means of a tool that periodically refreshes the data.

- Data Classification and Management:
  Corporate and military organizations use a variety of classification schemes. Many corporations use a data classification scheme to help secure the confidentiality and integrity of information. The typical information classification scheme has three categories: confidential, internal, and external. Information owners are responsible for classifying the information assets for which they are responsible. At least once a year, information owners must review information classifications to ensure the information is still classified correctly and the appropriate access controls are in place.

- Security Clearances:
  Corresponding to the data classification scheme is the personnel security clearance structure. In organizations that require security clearances, each user of data must be assigned a single authorization level that indicates the level of classification he or she is authorized to view. This is usually accomplished by assigning each employee to a named role, such as data entry clerk, development programmer, information security analyst, or even CIO.

- Management of Classified Data:
  Management of classified data includes its storage, distribution, portability, and destruction. All information that is not unclassified or public must be clearly marked as such. When classified data is stored, it must be available only to authorized individuals. This usually requires locking file cabinets, safes, or other protective devices for hard copies and systems. When a person carries classified information, it should be inconspicuous, as in a locked briefcase or portfolio.

- Classifying and Prioritizing Information Assets:
  Some organizations further subdivide the categories. For example, the category "Internet components" can be subdivided into servers, networking devices (routers, hubs, switches), protection devices (firewalls, proxies), and cabling. Each of the other categories can be similarly subdivided as needed by the organization. You should also include a dimension to represent the sensitivity and security priority of the data and the devices that store, transmit, and process the data—that is, a data classification scheme.

- Information Asset Valuation:
  To assign value to information assets for risk assessment purposes, you can pose a number of questions and collect your answers on a worksheet for later analysis. Before beginning the inventory process, the organization should determine which criteria can best establish the value of the information assets.

- Information Asset Prioritization:
  Once the inventory and value assessment are complete, you can prioritize each asset using a straightforward process known as weighted factor analysis. In this process, each information asset is assigned a score for each of a set of assigned critical factor.

Information Asset Valuation Example

System Name: SLS E-Commerce
Date Evaluated: February 2012
Evaluated By: D. Jones

Information assets	Data classification	Impact to profitability
Information Transmitted:		
EDI Document Set 1—Logistics BOL to outsourcer (outbound)	Confidential	High
EDI Document Set 2—Supplier orders (outbound)	Confidential	High
EDI Document Set 2—Supplier fulfillment advice (inbound)	Confidential	Medium
Customer order via SSL (inbound)	Confidential	Critical
Customer service request via e-mail (inbound)	Private	Medium
DMZ Assets:		
Edge router	Public	Critical
Web server #1—home page and core site	Public	Critical
Web server #2—Application server	Private	Critical

Notes: BOL: Bill of Lading
DMZ: Demilitarized Zone
EDI: Electronic Data Interchange
SSL: Secure Sockets Layer

Information Asset Prioritization Example

Information Asset	Criteria 1: Impact to Revenue	Criteria 2: Impact to Profitability	Criteria 3: Impact to Public Image	Weighted Score
Criterion Weight (1-100) Must total 100	30	40	30	
EDI Document Set 1—Logistics BOL to outsourcer (outbound)	0.8	0.9	0.5	75
EDI Document Set 2—Supplier orders (outbound)	0.8	0.9	0.6	78
EDI Document Set 2—Supplier fulfillment advice (inbound)	0.4	0.5	0.3	41
Customer order via SSL (inbound)	1.0	1.0	1.0	100
Customer service request via e-mail (inbound)	0.4	0.4	0.9	55

Identifying and Prioritizing Threats

After identifying and performing the preliminary classification of an organization's information assets, the analysis phase moves on to an examination of the threats facing the organization. A wide variety of threats face an organization and its information and information systems. The realistic threats must be investigated further while the unimportant threats are set aside. If you assume every threat can and will attack every information asset, the project scope quickly becomes so complex it overwhelms the ability to plan.

- Which threats present a danger to an organization's assets in the given environment?
  - Not all threats have the potential to affect every organization.
- Which threats represent the most danger to the organization's information?

  - The degree of danger a threat presents is difficult to assess.
- How much would it cost to recover from a successful attack?
  - One of the calculations that guides corporate spending on controls is the cost of recovery operations in the event of a successful attack.
- Which of the threats would require the greatest expenditure to prevent?
  - Just as in the previous question, another factor that affects the level of danger posed by a particular threat is the cost of protecting the organization against the threat.

Identifying Threats Example

Threat	Example
Compromises to intellectual property	Piracy, copyright infringement
Espionage or trespass	Unauthorized access and/or data collection
Forces of nature	Fire, flood, earthquake, lightning
Human error or failure	Accidents, employee mistakes, failure to follow policy
Information extortion	Blackmail of information disclosure
Missing, inadequate, or incomplete controls	Software controls, physical security
Missing, inadequate, or incomplete organizational policy or planning	Training issues, privacy, lack of effective policy
Quality of service deviations from service providers	Power and WAN quality of service issues
Sabotage or vandalism	Destruction of systems or information
Software attacks	Viruses, worms, macros, denial of service
Technical hardware failures or errors	Equipment failure
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies
Theft	Illegal confiscation of property

Vulnerability Identification

Once you have identified the organization's information assets and documented some criteria for beginning to assess the threats it faces, you then review each information asset for each threat it faces and create a list of vulnerabilities. What are vulnerabilities? They are specific avenues that threat agents can exploit to attack an information asset. They are chinks in the armor—a flaw or weakness in an information asset, security procedure, design, or control that could be exploited accidentally or on purpose to breach security.

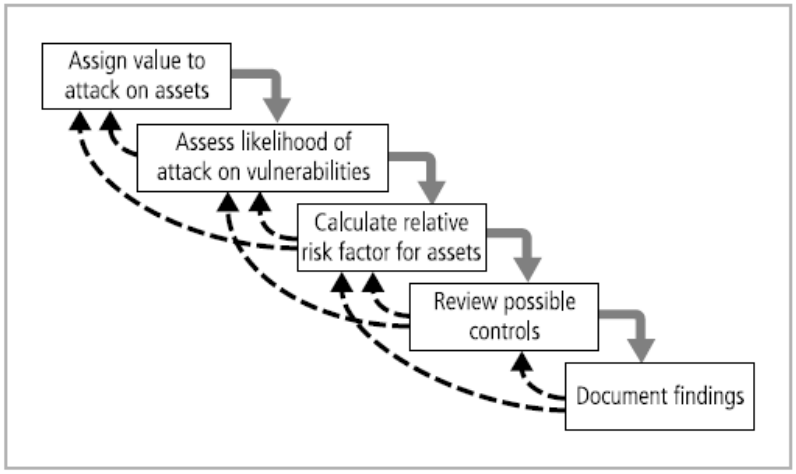
Week 08 – Topic 01

Risk Assessment

Now that you have identified the organization's information assets and the threats and vulnerabilities, you can evaluate the relative risk for each of the vulnerabilities. This process is called risk assessment. Risk assessment assigns a risk rating or score to each information asset.

While this number does not mean anything in absolute terms, it is useful in gauging the relative risk to each vulnerable information asset and facilitates the development of comparative ratings later in the risk control process.

Major Stages of Risk Assessment



Likelihood

Likelihood is the probability that a specific vulnerability will be the object of a successful attack. In risk assessment, you assign a numeric value to likelihood. The National Institute of Standards and Technology recommends (in Special Publication 800-30) assigning a number between 0.1 (low) and 1.0 (high).

For example, the likelihood of an asset being struck by a meteorite while indoors would be rated 0.1. At the other extreme, receiving at least one e-mail containing a virus or worm in the next year would be rated 1.0. You could also choose to use a number between 1 and 100 (zero is not used, since vulnerabilities with a zero likelihood have been removed from the asset/vulnerability list).

Whichever rating system you choose, use professionalism, experience, and judgment—and use the rating model you select consistently. Whenever possible, use external references for likelihood values that have been reviewed and adjusted for your specific circumstances. Many asset/vulnerability combinations have sources for likelihood, for example:

- The likelihood of a fire has been estimated actuarially for each type of structure.
- The likelihood that any given e-mail contains a virus or worm has been researched.
- The number of network attacks can be forecast based on how many assigned network addresses the organization has.

Risk Determination

For the purpose of relative risk assessment, risk *equals* likelihood of vulnerability occurrence *times* value (or impact) *minus* percentage risk already controlled *plus* an element of uncertainty, as illustrated in Figure.

Factors of Risk

Risk is
the **likelihood** of the occurrence of a vulnerability
multiplied by
the **value** of the information asset
minus
the percentage of risk mitigated by **current controls**
plus
the **uncertainty** of current knowledge of the vulnerability

For example:

- Information asset A has a value score of 50 and has one vulnerability. Vulnerability 1 has a likelihood of 1.0 with no current controls. You estimate that assumptions and data are 90 percent accurate.
- Information asset B has a value score of 100 and has two vulnerabilities: Vulnerability 2 has a likelihood of 0.5 with a current control that addresses 50 percent of its risk; vulnerability 3 has a likelihood of 0.1 with no current controls. You estimate that assumptions and data are 80 percent accurate.

The resulting ranked list of risk ratings for the three vulnerabilities is:

- Asset A: Vulnerability 1 rated as $55 = (50 \times 1.0) - 0\% + 10\%$ where
  $55 = (50 \times 1.0) - ((50 \times 1.0) \times 0.0) + ((50 \times 0.0) \times 0.1)$
  $55 = 50 - 0 + 5$
- Asset B: Vulnerability 2 rated as $35 = (100 \times 0.5) - 50\% + 20\%$ where
  $35 = (100 \times 0.5) - ((100 \times 0.5) \times 0.5) + ((100 \times 0.5) \times 0.2)$
  $35 = 50 - 25 + 10$
- Asset B: Vulnerability 3 rated as $12 = (100 \times 0.1) - 0\% + 20\%$ where
  $12 = (100 \times 0.1) - ((100 \times 0.1) \times 0.0) + ((100 \times 0.1) \times 0.2)$
  $12 = 10 - 0 + 2$

Identify Possible Controls

For each threat and its associated vulnerabilities that have residual risk, you must create a preliminary list of potential controls. *Residual risk* is the risk to the information asset that remains even after the application of controls.

Controls, safeguards, and countermeasures are terms for security mechanisms, policies, and procedures. These mechanisms, policies, and procedures counter attacks, reduce risk, resolve vulnerabilities, and otherwise improve the general state of security within an organization.

There are three general categories of controls:

1. Policies
2. Programs
3. Technologies

Policies are documents that specify an organization's approach to security. There are four types of security policies:

i. General security policies
ii. Program security policies
iii. Issue-specific policies
iv. Systems-specific policies

The *general security policy* is an executive-level document that outlines the organization's approach and attitude toward information security and relates the strategic value of information security within the

organization. This document, typically created by the CIO in conjunction with the CEO and CISO, sets the tone for all subsequent security activities.
The *program security policy* is a planning document that outlines the process of implementing security in the organization. This policy is the blueprint for the analysis, design, and implementation of security.
Issue-specific policies address the specific implementations or applications of which users should be aware. These policies are typically developed to provide detailed instructions and restrictions associated with security issues. Examples include policies for Internet use, e-mail, and access to the building.
Finally, *systems-specific policies* address the particular use of certain systems. This could include firewall configuration policies, systems access policies, and other technical configuration areas.

Programs are activities performed within the organization to improve security. These include security education, training, and awareness programs.

Security technologies are the technical implementations of the policies defined by the organization.
One particular approach to control is fundamental to the processes of information security.

Access control is often considered a simple function of the information system that uses it. In fact the principles of access control apply to physical control and other kinds of systems unrelated to IT.

Documenting the Results of Risk Assessment
By the end of the risk assessment process, you probably have in hand long lists of information assets with data about each of them. The goal so far has been to identify the information assets that have specific vulnerabilities and list them, ranked according to those most needing protection. In preparing this list, you collected and preserved a wealth of factual information about the assets, the threats they face, and the vulnerabilities they expose. You should also have collected some information about the controls that are already in place. The final summarized document is the ranked vulnerability risk worksheet, a sample of which is shown here:

Ranked Vulnerability Risk Worksheet

Asset	Asset Impact or Relative Value	Vulnerability	Vulnerability Likelihood	Risk-Rating Factor
Customer service request via e-mail (inbound)	55	E-mail disruption due to hardware failure	0.2	11
Customer order via SSL (inbound)	100	Lost orders due to Web server hardware failure	0.1	10
Customer order via SSL (inbound)	100	Lost orders due to Web server or ISP service failure	0.1	10
Customer service request via e-mail (inbound)	55	E-mail disruption due to SMTP mail relay attack	0.1	5.5
Customer service request via e-mail (inbound)	55	E-mail disruption due to ISP service failure	0.1	5.5
Customer order via SSL (inbound)	100	Lost orders due to Web server denial-of-service attack	0.025	2.5
Customer order via SSL (inbound)	100	Lost orders due to Web server software failure	0.01	1

The worksheet shown in Table is organized as follows:

- Asset: List each vulnerable asset.
- Asset Impact: Show the results for this asset from the weighted factor analysis worksheet. In the example, this is a number from 1 to 100.
- Vulnerability: List each uncontrolled vulnerability.
- Vulnerability Likelihood: State the likelihood of the realization of the vulnerability by a threat agent, as noted in the vulnerability analysis step. In the example, the number is from 0.1 to 1.0.
- Risk-Rating Factor: Enter the figure calculated from the asset impact multiplied by likelihood. In the example, the calculation yields a number from 1 to 100.

You may be surprised that the most pressing risk in Table lies in the vulnerable mail server. Even though the information asset represented by the customer service e-mail has an impact rating of only 55, the relatively high likelihood of a hardware failure makes it the most pressing problem.

Now that you have completed the risk identification process, what should the documentation package for this process look like? In other words, what are the deliverables from this phase of the project? The process you develop for risk identification should include designating what function the reports serve, who is responsible for preparing the reports, and who reviews them. The ranked vulnerability risk worksheet is the initial working document for the next step in the risk management process: assessing and controlling risk. Table below shows a sample list of the worksheets that might be prepared by the information security project team.

Risk Identification and Assessment Deliverables

Deliverable	Purpose
Information asset classification worksheet	Assembles information about information assets and their impact on or value to the organization
Weighted criteria analysis worksheet	Assigns ranked value or impact weight to each information asset
Ranked vulnerability risk worksheet	Assigns ranked value of risk rating for each uncontrolled asset-vulnerability pair

Week 08 – Topic 02

Risk Control Strategies

When organizational management determines that risks from information security threats are creating a competitive disadvantage, they empower the information technology and information security communities of interest to control the risks. Once the project team for information security development has created the ranked vulnerability worksheet, the team must choose one of five basic strategies to control each of the risks that result from these vulnerabilities. The five strategies are defend, transfer, mitigate, accept, and terminate.

- **Defend/Avoidance:** Apply safeguards that eliminate or reduce residual risks. (Residual risk is the risk to the information asset that remains even after the application of controls.)
- **Transference:** Transfer the risk to other areas or outside entities
- **Mitigation:** Reduce the impact of vulnerability exploitation
- **Acceptance:** Understand the consequences and accept the risk without control or mitigation.
- **Terminate:** directs the organization to avoid those business activities that introduce uncontrollable risks.

1. Defend / Avoidance

The defend control strategy attempts to prevent the exploitation of the vulnerability. This is the preferred approach and is accomplished by means of countering threats, removing vulnerabilities from assets, limiting access to assets, and adding protective safeguards.

There are three common methods used to defend:

- Application of policy
- Education and training
- Application of technology

Another defend strategy is the implementation of security controls and safeguards to deflect attacks on systems and therefore minimize the probability that an attack will be successful.

2. Transfer / Transference

The transfer control strategy attempts to shift risk to other assets, other processes, or other organizations. This can be accomplished by rethinking how services are offered, revising deployment models, outsourcing to other organizations, purchasing insurance, or implementing service contracts with providers. In end they stay reasonably close to the business they know and for risk control expertise, they rely on consultants or contractors.

Outsourcing, however, is not without its own risks. The owner of the information asset, IT management, and the information security team must ensure that the disaster recovery requirements of the outsourcing contract are sufficient and have been met before they are needed. If the outsourcer fails to meet the contract terms, the consequences may be far worse than expected.

3. Mitigate / Mitigation

The mitigate control strategy attempts to reduce the impact caused by the exploitation of vulnerability through planning and preparation.

This approach requires the creation of three types of plans: *the incident response plan, the disaster recovery plan, and the business continuity plan.*

Each of these plans depends on the ability to detect and respond to an attack as quickly as possible and relies on the quality of the other plans. Mitigation begins with the early detection that an attack is in progress and a quick, efficient, and effective response.

Summaries of Mitigation Plans

Plan	Description	Example	When Deployed	Time Frame
Incident Response Plan	Actions an organization takes during incidents (attacks)	• List of steps to be taken during disaster • Intelligence gathering • Information analysis	As incident or disaster unfolds	Immediate and real-time reaction
Disaster Recovery Plan	Preparations for recovery should a disaster occur; strategies to limit losses before and during disaster; step-by-step instructions to regain normalcy	• Procedures for the recovery of lost data • Procedures for the reestablishment of lost services • Shutdown procedures to protect systems and data	Immediately after the incident is labeled a disaster	Short-term recovery
Business Continuity Plan	Steps to ensure continuation of the overall business when the scale of a disaster exceeds the DR plan's ability to restore operations	• Preparation steps for activation of secondary data centers • Establishment of a hot site in a remote location	Immediately after the disaster is determined to affect the continued operations of the organization	Long-term operation

4. Accept / Acceptance

The accept control strategy is the choice to do nothing to protect a vulnerability and to accept the outcome of its exploitation. This may or may not be a conscious business decision. The only industry-recognized valid use of this strategy occurs when the organization has done the following:

- Determined the level of risk.
- Assessed the probability of attack.
- Estimated the potential damage that could occur from attacks.
- Performed a thorough cost benefit analysis.
- Evaluated controls using each appropriate type of feasibility.
- Decided that the particular function, service, information, or asset did not justify the cost of protection.

This strategy is based on the conclusion that the cost of protecting an asset does not justify the security expenditure. *Risk appetite* describes the degree to which organization is willing to accept risk as trade-off to the expense of applying controls.

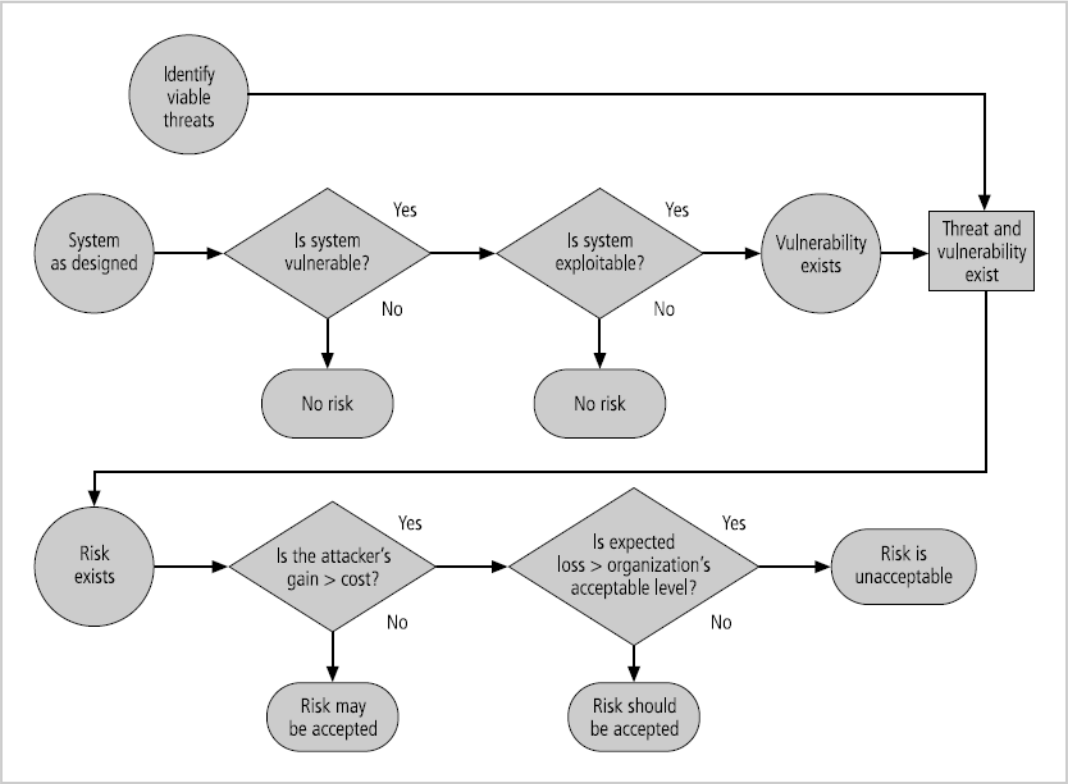
5. Terminate

The terminate control strategy directs the organization to avoid those business activities that introduce uncontrollable risks. If an organization studies the risks from implementing business-to-consumer e-commerce operations and determines that the risks are not sufficiently offset by the potential benefits, the organization may seek an alternate mechanism to meet customer needs—perhaps developing new channels for product distribution or new partnership opportunities. By terminating the questionable activity, the organization reduces the risk exposure.

Selecting a Risk Control Strategy

Risk control involves selecting one of the five risk control strategies for each vulnerability. The flowchart in figure guides you through the process of deciding how to proceed with one of the five strategies.

Risk Handling Decision Points



As shown in the diagram, after the information system is designed, you query as to whether the protected system has vulnerabilities that can be exploited. If the answer is yes and a viable threat exists, you begin to examine what the attacker would gain from a successful attack. To determine if the risk is acceptable or not, you estimate the expected loss the organization will incur if the risk is exploited. Some rules of thumb on strategy selection are presented below. When weighing the benefits of the different strategies, keep in mind that the level of threat and value of the asset should play a major role in strategy selection.

- When a vulnerability (flaw or weakness) exists: Implement security controls to reduce the likelihood of a vulnerability being exercised.
- When a vulnerability can be exploited: Apply layered protections, architectural designs, and administrative controls to minimize the risk or prevent occurrence.
- When the attacker's cost is less than his or her potential gain: Apply protections to increase the attacker's cost (e.g., use system controls to limit what a system user can access and do, thereby significantly reducing an attacker's gain).
- When potential loss is substantial: Apply design principles, architectural designs, and technical and nontechnical protections to limit the extent of the attack, thereby reducing the potential for loss.

Selecting a Risk Control Strategy Phases

Feasibility Studies

Before deciding on the strategy (defend, transfer, mitigate, accept, or terminate) for a specific vulnerability, the organization must explore all the economic and noneconomic consequences of the vulnerability facing the information asset. This is an attempt to answer the question, "What are the actual and perceived advantages of implementing a control as opposed to the actual and perceived disadvantages of implementing the control?" There are a number of ways to determine the advantage of a specific control. There are also many methods an organization can use to identify the disadvantages of specific controls. *Cost avoidance* is the process of preventing the financial impact of an incident by implementing a control.

Cost Benefit Analysis (CBA)

Organizations must consider the economic feasibility of implementing information security controls and safeguards. While a number of alternatives for solving a problem may exist, they may not all have the same economic feasibility. Most organizations can spend only a reasonable amount of time and money on information security, and the definition of reasonable differs from organization to organization and even from manager to manager. Organizations are urged to begin the cost benefit analysis by evaluating the worth of the information assets to be protected and the loss in value if those information assets were compromised by the exploitation of a specific vulnerability. It is only common sense that an organization should not spend more to protect an asset than the asset is worth. The formal decision making process is called a cost benefit analysis or an economic feasibility study.

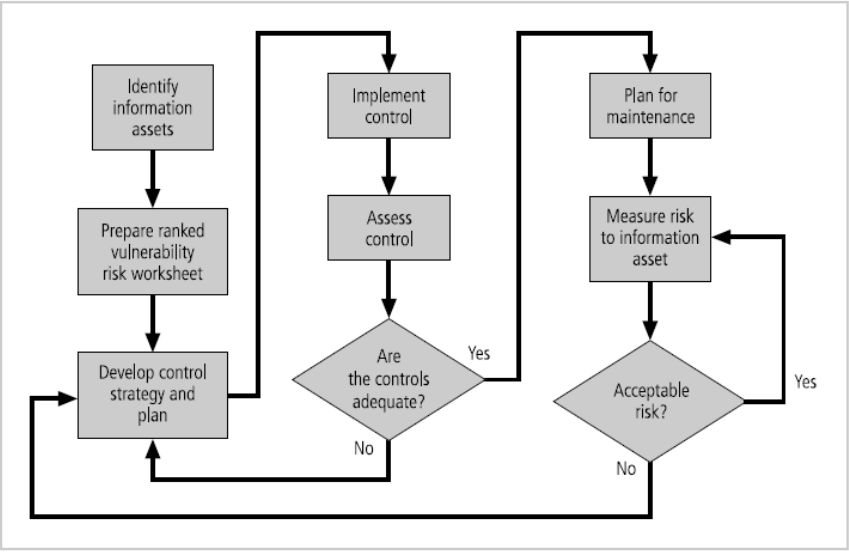
The Cost Benefit Analysis (CBA) Formula is:

$$CBA = ALE\ (prior) - ALE\ (post) - ACS$$

Where Annualized loss Expectancy is ALE and Annualized cost of Safeguard is ACS.

Evaluation, Assessment, and Maintenance of Risk Controls

The selection and implementation of a control strategy is not the end of a process; the strategy, and its accompanying controls, must be monitored and reevaluated on an ongoing basis to determine their effectiveness and to calculate more accurately the estimated residual risk. It is a process that continues for as long as the organization continues to function.



Quantitative Versus Qualitative Risk Control Practices

Step performed using actual values or estimates is known as a *quantitative assessment*. However, an organization could decide that it cannot put specific numbers on these values. Fortunately, it is possible to repeat these steps using an evaluation process, called *qualitative assessment* that does not use numerical measures. This could be accomplished using scales rather than specific estimates. A sample scale could include none, representing no chance of occurrence, then low, medium, high, up to very high, representing almost certain occurrence. Organizations may, of course, prefer other scales: A–Z, 0–10, 1–5, or 0–20. Using scales also relieves the organization from the difficulty of determining exact values. Many of these same scales can be used in any situation requiring a value, even in asset valuation.

Benchmarking

Instead of determining the financial value of information and then implementing security as an acceptable percentage of that value, an organization could take a different approach to risk management and look to peer organizations for benchmarks. Benchmarking is the process of seeking out and studying the practices used in other organizations that produce results you would like to duplicate in your organization. An organization typically benchmarks itself against other institutions by selecting a measure upon which to base the comparison. The organization then measures the difference between the way it conducts business and the way the other organizations conduct business.

Disadvantages:

- No sharing of attacks and lesson learned.
- No two organizations are identical.

<u>Other Feasibilities</u>

Organizational Feasibility:

Organizational feasibility analysis examines how well the proposed information security alternatives will contribute to the efficiency, effectiveness, and overall operation of an organization.

Operational Feasibilities:

Operational feasibility analysis examines user acceptance and support, management acceptance and support, and the overall requirements of the organization's stakeholders. Operational feasibility is also known as *behavioral feasibility*, because it measures the behavior of users.

Technical Feasibility:

Technical feasibility analysis examines whether or not the organization has or can acquire the technology necessary to implement and support the proposed control. Technical feasibility also examines whether the organization has the technological expertise to manage the new technology.

Political Feasibility:

Political feasibility determines what can and cannot occur based on the consensus and relationships among the communities of interest. The limits placed on an organization's actions or behaviors by the information security controls must fit within the realm of the possible before they can be effectively implemented, and that realm includes the availability of staff resources.