UNIT I

INTRODUCTION

History, What is Information Security?, Critical Characteristics of Information, NSTISSC Security Model, Components of an Information System, Securing the Components, Balancing Security and Access, The SDLC, The Security SDLC

PART A

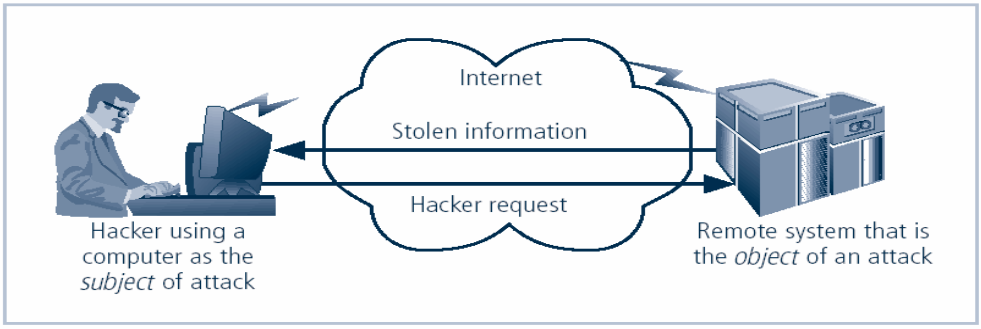
1. **What is information security? (May/June 2013, Nov/Dec 2011, May/June 2015,Nov/Dec 2012)**
    - Information security is the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information.
    - Tools, such as policy, awareness, training, education, and technology are necessary
2. **Why is a methodology important in implementing the information security? (Nov/Dec 2011)**
    - First, it entails all the rigorous steps for the organizations' employees to follow, therefore avoiding any unnecessary mistakes that may compromise the end goal.
    - Second, methodology increases the probability of success. Once a methodology is adopted, the personnel selected will be responsible for establishing key milestones and made ac-countable for achieving the project goals.
3. **Why is information security a management problem? (May/June 2014)**

    Information security is a concern of management as it is the responsibility of both the general management and the IT management. This is because it has to do both with policies passed and their enforcement and technology. Information security management systems are policies that are concerned with information security management and are formulated as part of the general management policies.
4. **What are the critical characteristics of information? (May/June 2013)**
    - Availability
    - Accuracy
    - Authenticity
    - Confidentiality
    - Integrity
    - Utility
    - Possession
5. **What does it mean to discover an exploit? How does an exploit differ from vulnerability? (MAY/JUNE 2014, NOV/DEC 2014, APRIL/MAY 2015)**

Exploit – Hackers may attempt to exploit a system or information by using it illegally. It can be a targeted solution to misuse a specific hole or vulnerability.

Vulnerability – Weaknesses or faults in a system or protection mechanism that expose information to attack or damage is called as vulnerability. They have been examined documented and published are referred as well known vulnerabilities.

6. **What are the multiple layers of security? (Nov/Dec 2012)**
   - Physical Security
   - Personal Security
   - Operations Security
   - Communication Security
   - Network Security
   - Information Security
7. **When can a computer be a subject and an object of an attack respectively? (Nov/Dec 2012)**
   - A **subject** is an active entity which interacts with information system and can be an individual, technical component or computer process.
   - An **object** is a passive entity that receives or contains information and they are assigned with specific controls that restrict or prevent access by unauthorized subjects.



FIGU **ıputer as the Subject and Object of an Attack**

8. **Why C.I.A triangle is commonly used in information security? (MAY/JUNE 2014)**

   The C.I.A. triangle - confidentiality, integrity, and availability - has expanded into a more comprehensive list of critical characteristics of information. At the heart of the study of information security is the concept of policy. Policy, awareness, training, education, and technology are vital concepts for the protection of information and for keeping information systems from danger.
9. **Write a note on the history of information security**
   - Computer security began immediately after the first mainframes were developed
   - Groups developing code-breaking computations during World War II

created the first modern computers

- Physical controls were needed to limit access to authorized personnel to sensitive military locations
- Only rudimentary controls were available to defend against physical theft, espionage, and sabotage

10. What is NSTISSC Security model? (May/June 2012)

This refers to "The National Security Telecommunications and Information Systems Security Committee" document. This document presents a comprehensive model for information security. The model consists of three dimensions.

11. Mention the components of information security. (APRIL/MAY 2014, NOV/DEC 2012)

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

12. How is the top down approach to information security superior to bottom up approach? (APR/MAY 2010)

The top down approach has the higher probability of success. In this approach the project is initiated by upper level managers who will issue policy, procedures and processes dictate the goals and expected outcomes of the project and also determine who is accountable for each of the required actions.

13. Define e-mail Spoofing. (APRIL/MAY 2014,APRIL/MAY 2015)

Email spoofing is the creation of **email** messages with a forged sender address. It is easy to do because the core protocols do not have any mechanism for authentication. It can be accomplished from within a LAN or from an external environment using Trojan horses.

PART B

1) Explain in detail about critical characteristics of information. (Nov/Dec 2011, May/June 2012, Nov/Dec 2012, May/June 2014)

Availability

- Availability enables users who need to access information to do so without interference or obstruction, and to receive it in the required format.
- Availability of information
    - ✓ Is accessible to any user.
    - ✓ Requires the verification of the user as one with authorized access to the information.
- The information, then, is said to be available to an authorized user when and where needed and in the correct format.

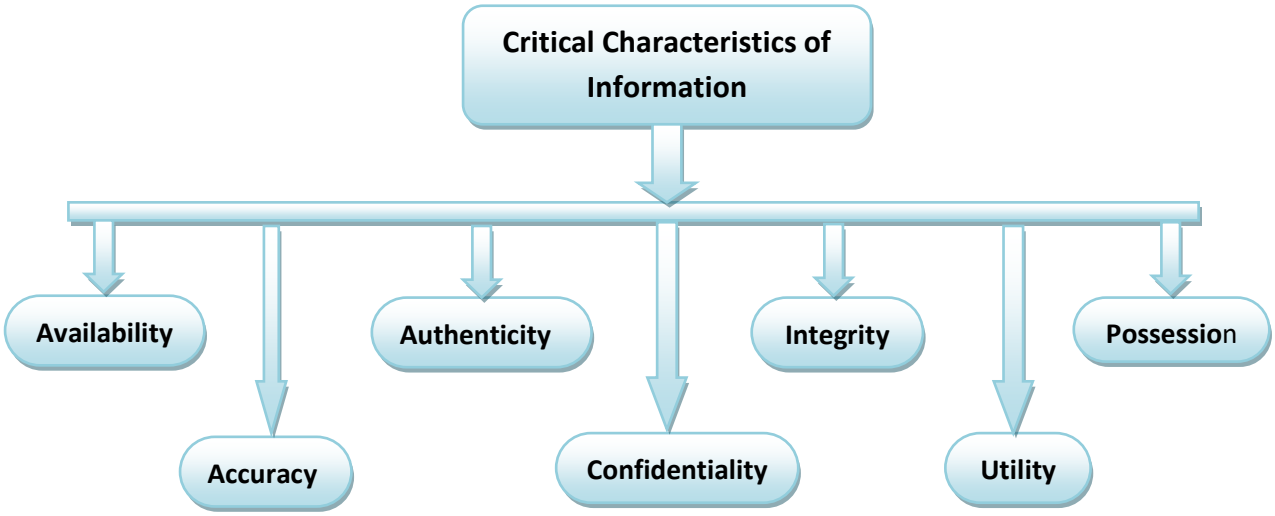


Fig: Critical Characteristics of Information

Example:-

Consider the contents of a library

- Research libraries that require identification before entrance.
- Librarians protect the contents of the library, so that it is available only to authorized patrons.
- The librarian must see and accept a patron's proof of identification before that patron has free and easy access to the contents available in the bookroom.

Accuracy

Information is accurate

- ✓ when it is free from mistakes or errors and
- ✓ It has the value that the end user expects.

Information contains a value different from the user's expectations due to the intentional or unintentional modification of its content, it is no longer accurate.

Example:-

Consider the checking account

- Inaccuracy of the information in your checking account can be caused by external or internal means.
- If a bank teller, for instance, mistakenly adds or subtracts too much from your account, the value of the information has changed.
- In turn, as the user of your bank account, you can also accidentally enter an incorrect amount into your account register. This also changes the value of the information.

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 the information that was originally
  - ✓ Created,
  - ✓ Placed,
  - ✓ Stored, or
  - ✓ Transferred.

Example:-

Consider for a moment some of the assumptions made about e-mail.

- ✓ When you receive e-mail, you assume that a specific individual or group of individuals created and transmitted the e-mail—you assume know the origin of the e-mail. This is not always the case.
- ✓ E-Mail spoofing, the process of sending an e-mail message with a modified field, is a problem for many individuals today, because many times the field modified is the address of the originator.
- ✓ Spoofing the address of origin can fool the e-mail recipient into thinking that the message is legitimate traffic.
- ✓ In this way, the spoofed can induce the e-mail readers into opening e-mail they otherwise might not have opened.
- ✓ The attack known as spoofing can also be applied to the transmission of data across a network, as in the case of user data protocol (UDP) packet spoofing, which can enable unauthorized access to data stored on computing systems.

Confidentiality

- The confidentiality of information is the quality or state of preventing disclosure or exposure to unauthorized individuals or systems.
- Confidentiality of information is ensuring that only those with the rights and privileges to access a particular set of information are able to do so, and that those who are not authorized are prevented from obtaining access.

- When unauthorized individuals or systems can view information, confidentiality is breached.
- To protect the confidentiality of information, you can use a number of measure:
  - ✓ Information classification
  - ✓ Secure documents storage
  - ✓ Application of general security policies
  - ✓ Education of information custodians and end users

Example:-

Ex: 1 A security is an employee throwing away a document containing critical information without shredding it.

Ex: 2 A hacker who successfully breaks into an internal database of a Web-based organization and steals sensitive information about the clients such as

- ✓ Names
- ✓ Addresses and
- ✓ Credit card numbers.

Integrity

- The quality or state of being whole, complete, and uncorrupted is the integrity of information.
- The integrity of information is threatened when the information is exposed to
  - ✓ Corruption,
  - ✓ Damage,
  - ✓ Destruction, or
  - ✓ Other disruption of its authentic state.
- The threat of corruption can occur while information is being stored or transmitted.
- Many computer viruses and worms have been created with the specific purpose of corrupting data.

For this reason the key method for detecting the virus or worm

1. First Key methodology is to look for changes in file integrity as shown by the size of the file.
2. Another key methodology for assuring information integrity is through file hashing.
   - ✓ With file hashing, 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 different for each combination.

Utility

• The Utility information is the quality or state of having value for some purpose or end.

• Information has value when it serves a particular purpose. This means that if information is available, but not in a format meaningful to the end user, it is not useful.

Possession

• The Possession of information is the quality or state of having ownership or control of some object or item.

• Information is said to be in possession if one obtains it, independent of format or other characteristic.

• A breach of confidentiality always results in a breach of possession, a breach of possession does not always result in a breach of confidentiality.

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, 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.

2) Explain the NSTISSC Security model and the approaches used for security implementation. (NOV/DEC 2011, NOV/DEC 2012)

NSTISSC Security Model

- The definition for information security presented earlier which is based in part on the National Security Telecommunications and Information Systems Security Committee document called the **National Training Standard for Information Security Professionals NSTISSI No.4011**
- This document presents a **comprehensive model** for information security and is becoming the **evaluation standard** for the security of information systems.

The security model, as represented in figure shows the three dimensions

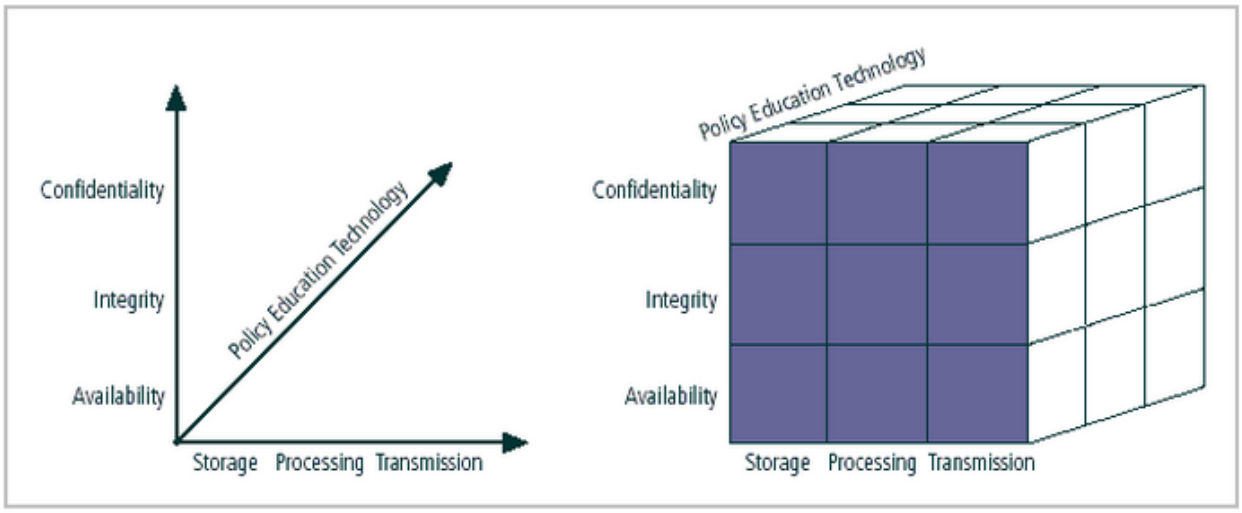
- If you extrapolate the three dimensions of each axis, you end up with a 3×3×3 cube with 27 cells representing areas that must be addressed to secure the information systems of today.
- Your primary responsibility is to make sure that each of the 27 cells is properly addressed during the security process.

For example

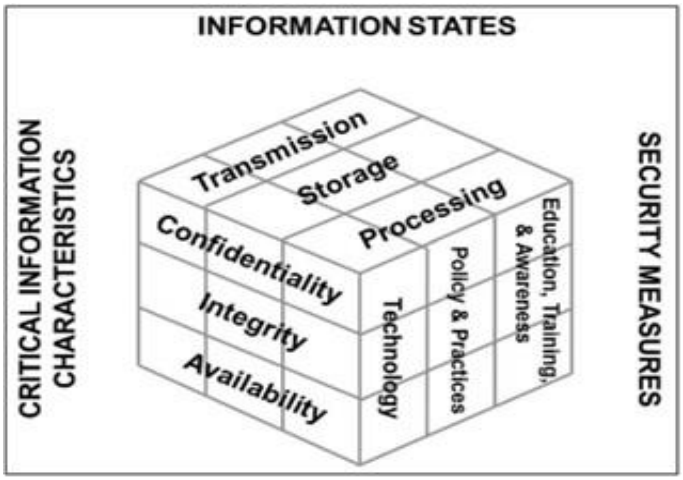
- If you look at the intersection between
    - The technology,
    - Integrity, and
    - Storage areas.
- You would expect to see a control or safeguard that indicates that you have addressed the need to use technology to protect the integrity of information while in storage.
- One technology you could use would be a **system to detect host intrusion** that is designed to **protect the integrity** of information by alerting the security administrators of the potential modification of a critical file.
- Your job is to examine all cells, and make sure each is addressed to your satisfaction.
- What is commonly left out of such a model is the need for guidelines and policies that provide direction for the practices and implementations of technologies.
- The information system has its own security requirements

.

[NSTISSC Security model]

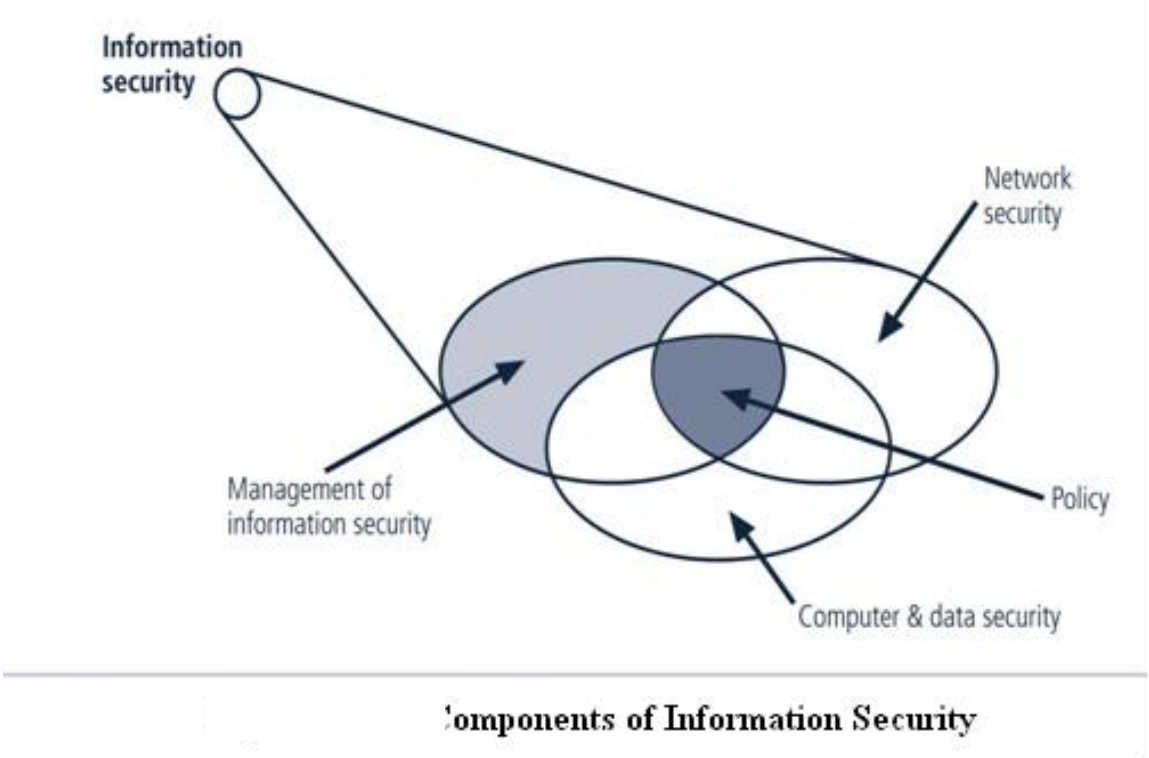


The C.I.A. triangle - confidentiality, integrity, and availability - has expanded into a comprehensive list of critical



more

characteristics of information. At the heart of the study of information security is the concept of policy. Policy, awareness, training, education, and technology are vital concepts for the protection of information and for keeping information systems from danger



Components of Information Security

Approaches to Information Security Implementation

Securing information assets is in fact an incremental process that requires coordination, time, and patience. Information security can begin as a grassroots effort in which systems administrators attempt to improve the security of their systems. This is often referred to as a **bottom-up approach**. The key advantage of the bottom-up approach is the technical expertise of the individual administrators.

The **top-down approach** in which the project is initiated by upper-level managers who issue policy, procedures and processes, dictate the goals and expected outcomes, and determine accountability for each required action has a higher probability of success. This approach has strong upper-management support, a dedicated champion, usually dedicated funding, a clear planning and implementation process, and the means of influencing organizational culture.

The top down and bottom up approaches will include the following:

1. It has higher probability of success.

2. Project is initiated by upper level managers who issue policy & procedures & processes.

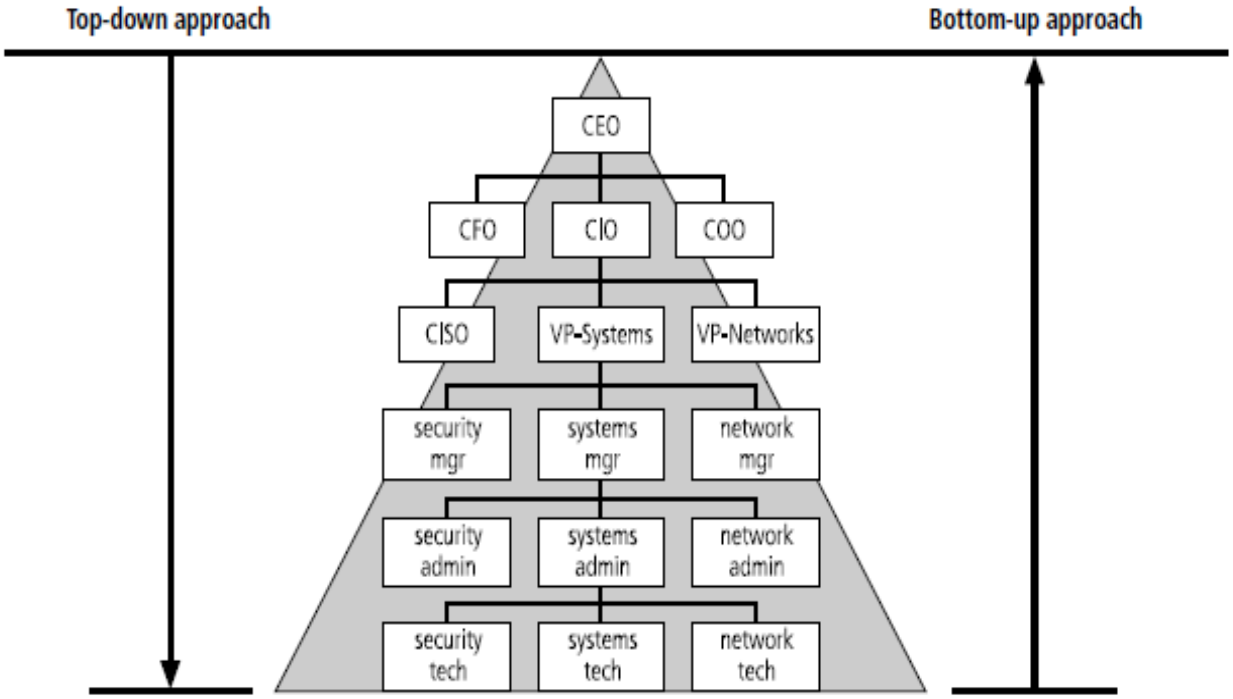
3. Dictate the goals & expected outcomes of the project.

4. Determine who is suitable for each of the required action.

Balancing Information 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. To achieve balance it is to operate an information system that satisfies the user and the security professional with the security level must allow reasonable access. An imbalance can occur when the needs of the end user are undermined by too heavy a focus on protecting and administering the information systems.

Both information security technologists and end users must recognize that both groups share the same overall goals of the organization to ensure the data is available when, where, and how it is needed, with minimal delays or obstacles. In an ideal world, this level of availability can be met even after concerns about loss, damage, interception, or destruction have been addressed.



3) Write in detail about the components of an information system (Nov /Dec 2011, May/June 2015, Nov/Dec 2014, Nov/Dec 2012, May/June 2013)

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

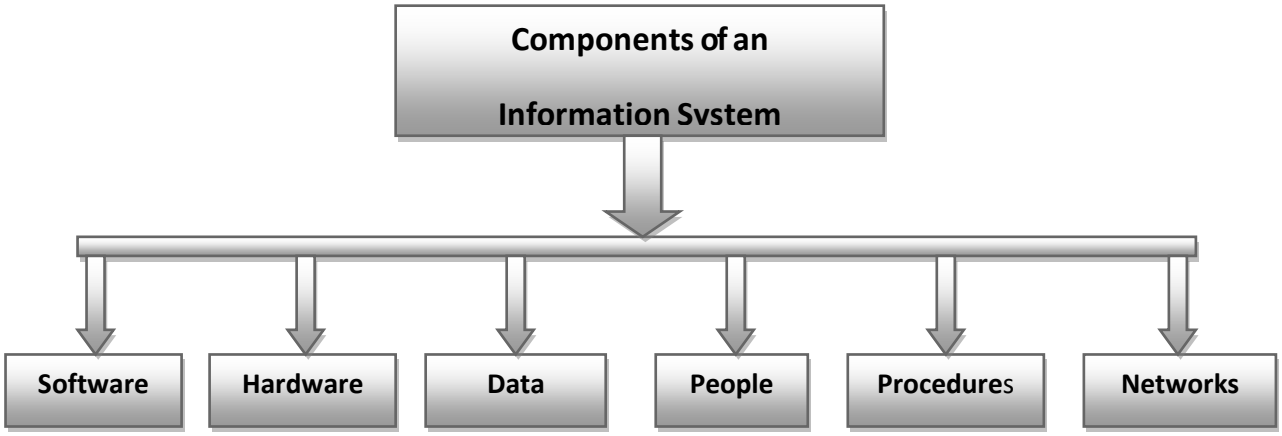


Fig: Components of an Information System

- These are the six **critical components.**
- Each of these six components has its own strengths and weaknesses – its own characteristics and uses.
- Each component of the information system has its own **security requirements.**

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.
- Exploiting errors in software programming results in a substantial portion of the attacks on information.
- The news is filled
  - With reports warning of holes,
  - Bugs
  - Weaknesses or
  - Other fundamental problems in software.
- Software programs are the vessels that carry the lifeblood of information through an organization.
- Software programs are often created under the demanding constraints of project management
  - Time
  - Cost &
  - Manpower.

Hardware

- It is the physical technology that houses and executes the software, stores and carries the data, and provides interfaces for the entry and removal of information from the system.
- Physical security policies deal with hardware as a physical asset and with the protection of these physical assets from harm or theft.
- We can apply the traditional tools of physical security such as **locks and keys**, to restrict access to and interaction of computers

Data

- It is evident that
  - Data stored
  - Processed, and
  - Transmitted through a computer system must be protected.
- Data is usually the main object of intentional attacks.

People

- People are often a threat to information security.
- Legend has it that around 200 B.C., a great army threatened the security and stability of the Chinese empire. So ferocious were the invaders that the Chinese emperor commanded the construction of a great wall that would defend against the Hun invaders.
- Around $1275_{A.D.}$ Kublai Khan finally achieved what the Huns had been trying for thousands of years. Initially, the Khan's army tried to climb over, dig under, and break through the wall.

Procedures

- Procedures are written instructions for accomplishing a specific task.
- If an unauthorized user obtains an organization's procedures, a threat to the integrity of the information is posed.

For example

- A consultant of a bank learned how to wire funds by using the computer center's procedures that 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 an unauthorized account.
- Lax security of the information system caused the loss of over ten million dollars before the situation was corrected.
- Most organizations focus on distributing procedures to their legitimate employees, so that they can access the information system. How – ever, proper education on the protection of those procedures is often lacking.

Networks

- ✓ When information systems are connected to each other to form Local Area Network (LANs), and these LANs are connected to other networks such as the Internet, new security challenges rapidly emerge.
- ✓ Steps to provide network security are essential, as is the

implementation of alarm and intrusion systems to make system owners aware of ongoing compromises.

Components of an Information System - Summary

Hardware	**It** is the physical technology that houses and executes the software, stores and carries the data, provides interfaces for the entry and removal of information from the system.
Software	**It is a component** of IS comprises applications, operating systems, and assorted command utilities.
People	Though often overlooked in computer security considerations, people have always been a threat to information security and they are the weakest link in a security chain
Procedures	They are written instructions for accomplishing when an unauthorized user obtains an organization's procedures; it poses threat to the integrity of the information.
Data	Data stored, processed, and transmitted through a computer system must be protected. Data is the most valuable asset possessed by an organization and it is the main target of intentional attacks.
Networks	Information systems in LANs are connected to other networks such as the internet and new security challenges are rapidly emerge.

4) What is SDLC? Explain the different phases of SDLC. (May/June 2015, Nov/Dec 2014, May/June 2014, May/June 2013)

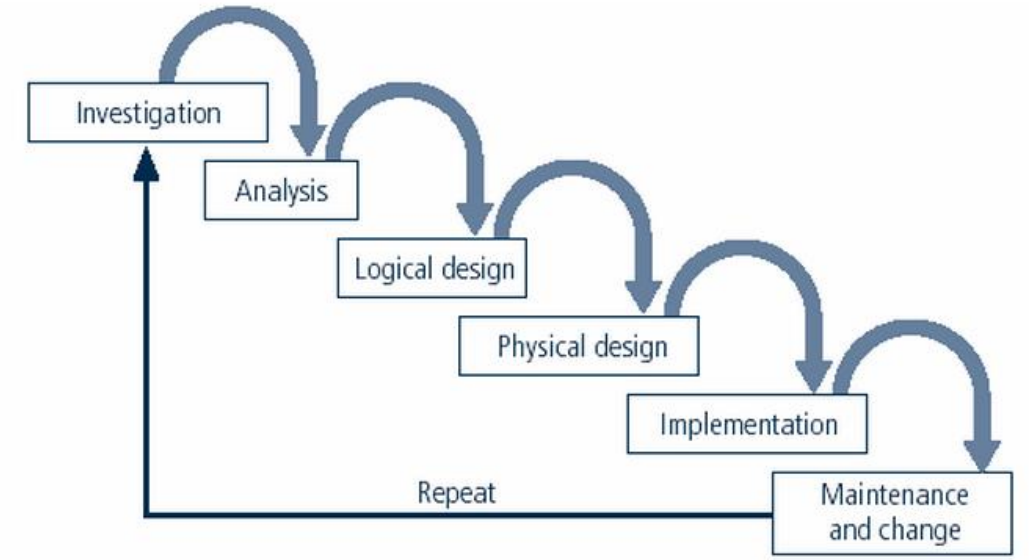
Methodology

- The SDLC is a methodology for the design and implementation of an information system in an organization.
- A methodology is a formal approach to solving a problem based on a structured sequence of procedures.
- Using a methodology ensures a rigorous process and avoids missing those steps that can lead to compromising the end goal.
- The goal in this case is creating a comprehensive security posture.
- A methodology also 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 to accomplish the project goals.

SDLC Waterfall Methodology

Phases

- The traditional SDLC consists of six general phases.
- The different variations of SDLC range from three to 12 stages, all of which have been mapped into the six presented here.
- Each of these stages come from the Waterfall model pictured in Figure, in which each phase begins with the results and information gained from the previous phase.



SDLC Waterfall Methodology

- In the **Investigation phase**
  - The process begins with an investigation of the problem facing the organization
  - Analysis of current organizational practices considered in the context of the investigation
- Then proceeds into the **logical and physical design phases**.

- During the **design phases** potential solutions are identified and are associated with evaluation criteria.
- In the **implementation phase**
  - Solutions are evaluated
  - Selected, and
  - Acquired through a make-or-buy process.

These solutions, whether made or bought, are tested, installed, and tested again. Users of systems are trained and documentation developed.

- Finally, the system becomes mature and is **maintained** and modified over the remainder of its operational life.

Investigation

In the Investigation phase

- What is the problem the system is 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 is specified.
- A preliminary cost benefit analysis is developed to evaluate the perceived benefits and the appropriate levels of cost for those benefits.
- At the conclusion of this stage a feasibility analysis is performed which
  - Assesses the economic
  - Technical and
  - Behavioral feasibilities of the process and ensures that implementation is worth the organization's time and effort.

Analysis

- The analysis phase begins with the information gained during the investigation phase.
- This phase consists
  - Primarily of assessments of the organization,
  - The status of current systems, and
  - The capability to support the proposed systems.
- Analysts begin to determine
  - What the new system is expected to do and
  - How it will interact with existing systems.
- This phase ends with the documentation of the findings and an update of the feasibility analysis.

Logical Design

- The information gained from the analysis phase is used to begin creating a solution system for a business problem.
- In any systems solution, it is imperative that the first and driving factor is the business need.
- Then, based on the business need applications are selected that are capable of providing needed services.
- Based on the applications needed, **data support and structures** capable of providing the needed inputs are then chosen.
- 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, meanings that it contains no reference to **specific technologies, vendors, or products**.

Physical Design

- The 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.
- Final designs integrate various components and technologies. After yet another feasibility analysis, the entire solution is presented to the organizational management for approval.

Implementation

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

Maintenance and Change

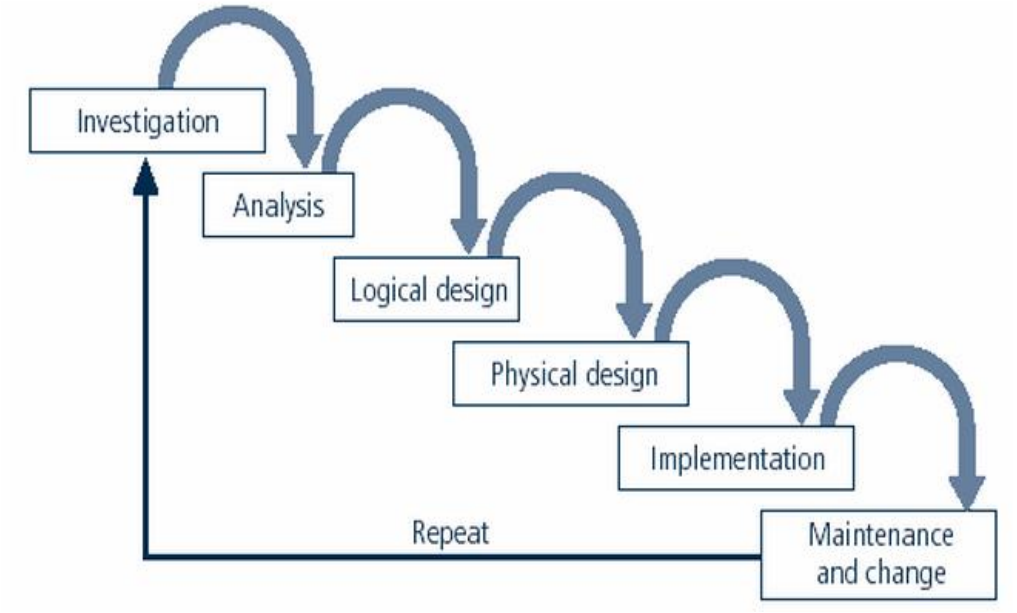
- The maintenance and change phase is the longest and most expensive phase of the process.
- This phase consists of
  - The tasks necessary to support and
  - Modify the system for the remainder of its useful life cycle.
- Even though formal development may conclude during this phase, the life cycle 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.

- When the current system can no longer support the evolving mission of the organization, the project is terminated and a new project is implemented.

5) What is Security SDLC? Explain its different phases. (Nov /Dec 2011, Nov/Dec 2014, Nov/Dec 2012, May/June 2013)



Security SDLC

Investigation

- The investigation of the Sec SDLC 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
  - A statement of program security policy that outlines the implementation of a security program within the organization.
  - Teams of responsible managers, employees, and contractors are organized,
  - Problems analyzed, and scope defined, including specific goals and objectives.
  - Finally, an organizational feasibility analysis is performed to determine whether the organization has the resource 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 created during the investigation phase
  - Conducts a preliminary analysis of existing security policies or programs.
  - Along with documented current threats and associated controls.
- This phase also includes an analysis of relevant legal issues that could impact the design of the security solution.

- Increasingly, privacy laws have become a major consideration when making decisions about information systems that manage personal information.
- The risk management task also begins in this stage.

Risk management is the process of

- Identifying
- Assessing &
- 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 security and
- Examines and implements key policies that influence later decisions.

- Also at this stage, **critical planning** is developed for 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 do you do when an attack occurs?
- Disaster recovery : What must you do to recover information and vital Systems immediately after a disastrous event?

- These questions are examined and solutions documented.
- Next, a feasibility analysis determines whether or not the project should continue or should be outsourced.

Physical Design

In the physical design phase,

- The security technology needed to support
  - The blueprint outlined in the logical design is evaluated
  - Alternative solutions generated, and
  - A final design agreed upon.
- The security blueprint may be revisited to keep it in line with the changes needed when the physical design is completed.
- Criteria needed to determine 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 should determine 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 is similar to the traditional SDLC.
- The security solutions are
  - Acquired
  - 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

The maintenance and change phase

- Today's information security systems need
  - Constant monitoring,
  - Testing
  - Modification
  - Updating and
  - Repairing.

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 process 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	♦ Analyze existing security policies and programs ♦ Analyze current threats and controls ♦ Examine legal issues ♦ Perform risk analysis.

	feasibility analysis.	
Phase 3: **Logical Design**	♦ Assess current business needs against plan developed in Phase 2 ♦ Select applications, data support, and structures ♦ Generate multiple solutions for consideration ♦ Document findings and update feasibility analysis.	♦ Develop security blueprint ♦ Plan incident response actions ♦ Plan business response to disaster ♦ Determine feasibility of continuing and/or outsourcing the project.
Phase 4: **Physical Design**	♦ Select technologies to support solutions developed in Phase 3 ♦ Select the best solution ♦ Decide to make or buy components ♦ Document findings and update feasibility analysis.	♦ Select technologies needed to support security blueprint ♦ Develop definition of successful solution ♦ Design physical security measures to support technological 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**	♦ 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.

6) **List and discuss about the role and focus of professional organizations in providing information security. (MAY/JUNE 2013, NOV/DEC 2014)**

Security Professionals and the organization

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. The roles of information security professionals are aligned with the goals and mission of the information security community of interest. These job functions and organizational roles focus on protecting the organization's information systems and stored information from attacks.

Senior management

The CIO is primarily responsible for advising the chief executive officer, president, or company owner on the strategic planning that affects the management of information in the organization. The CIO translates the strategic plans of the organization as a whole into strategic information plans for the information systems or data processing division of the organization. Once this is accomplished, CIOs work with subordinate managers to develop tactical and operational plans for the division and to enable planning and management of the systems that support the organization.

The chief information security officer (CISO) has primary responsibility for the assessment, management, and implementation of information security in the organization. The CISO may also be referred to as the manager for IT security, the security administrator. The CISO usually reports directly to the CIO, although in larger organizations it is not uncommon for one or more layers of management to exist between the two. However, the recommendations of the CISO to the CIO must be given equal, if not greater, priority than other technology and information-related proposals. Chief information Officer (CIO) is the responsible for the following:

1. Assessment
2. Management
3. Implementation of information security in the organization

Information Security Project Team

The information security project team should consist of a number of individuals who are experienced in one or multiple facets of the required technical and nontechnical areas. Members of the security project team fill the following roles:

- **Champion**: A senior executive who promotes the project and ensures its support, both financially and administratively, at the highest levels of the organization.
- **Team leader**: A project manager, who may be a departmental line manager or staff unit manager, who understands project management, personnel management, and information security technical requirements.

- **Security policy developers**: People who understand the organizational culture,existing policies, and requirements for developing and implementing successful policies.
- **Risk assessment specialists**: People who understand financial risk assessment techniques,the value of organizational assets, and the security methods to be used.
- **Security professionals**: Dedicated, trained, and well-educated specialists in all aspects of information security from both a technical and nontechnical standpoint.
- **Systems administrators**: People with the primary responsibility for administering the systems that house the information used by the organization.
- **End users**: Those whom the new system will most directly affect. Ideally, a selection of users from various departments, levels, and degrees of technical knowledge assist the team in focusing on the application of realistic controls applied in ways that do not disrupt the essential business activities they seek to safeguard.

Data Responsibilities

The three types of data ownership and their respective responsibilities are as follows:

Data owners

They are responsible for the security and use of a particular set of information. They are usually members of senior management and could be CIOs. The data owners usually determine the level of data classification (discussed later), as well as the changes to that classification required by organizational change. The data owners work with subordinate managers to oversee the day-to-day administration of the data.

Data custodians

Working directly with data owners, data custodians are responsible for the storage, maintenance, and protection of the information. Depending on the size of the organization, this may be a dedicated position, such as the CISO, or it may be an additional responsibility of a systems administrator or other technology manager. The duties of a data custodian often include overseeing data storage and backups, implementing the specific procedures and policies laid out in the security policies and plans, and reporting to the data owner.

Data users

End users who work with the information have to perform their assigned roles supporting the mission of the organization. Everyone in the organization is responsible for the security of data, so data users are included here as individuals with an information security role.

UNIT II

SECURITY INVESTIGATION

Need for Security, Business Needs, Threats, Attacks, Legal, Ethical and Professional Issues

PART A

1) Differentiate worm and viruses. (May/June 2012)

VIRUS	WORM
A virus attaches itself to s a computer program and spreads from one computer to another.	A worm is similar to virus by design. It also spreads from one computer to another.
Spreads with uniform speed as programmed.	Worms spread more rapidly than virus.
It can be attached to .EXE, .COM , .XLS etc	It can be attached to any attachments of email or any file on network.
Ex Melisca, cascade	Ex Blaster Worm
It requires the spreading of an infected host file.	It replicates them without the host file.

2) What are threats to information security? (May/June 2015, Nov/Dec 2012)

- A threat is an object, person, or other entity that represents a constant danger to an asset
- Management must be informed of the various kinds of threats facing the organization
  - ✓ Acts of Human error or failure.
  - ✓ Compromises to Intellectual Property
  - ✓ Deliberate acts of espionage or trespass
  - ✓ Deliberate acts of information extortion

- ✓ Deliberate acts of sabotage and vandalism
- ✓ Deliberate acts of theft
- ✓ Deliberate Software Attacks
- ✓ Forces of Nature
- ✓ Deviations in quality of service from service providers
- ✓ Technical Hardware Failures or Errors
- ✓ Technical Software Failures or Errors
- ✓ Technological Obsolescence

3) What are the general categories of unethical and illegal behavior? (Nov/Dec 2014, Nov/Dec2012)

There are three general categories of unethical and illegal behavior that organizations and society should seek to eliminate:

- Ignorance
- Accident
- Intent

4) What is Intellectual property? (May/June 2015,May/June 2013, Nov /Dec 2011)

Intellectual property is "the ownership of ideas and control over the tangible or virtual representation of those ideas". Many business organizations have to create intellectual property for :

- ❖ trade secrets
- ❖ copyrights
- ❖ trademarks
- ❖ patents

5) What is malware? What are it types? (May/June 2012)

Malware is software that does not benefit the computer's owner, and may even harm it, and so is purely parasitic. This kind of attack includes the execution of viruses, worms, Trojan horses, and active web scripts with the intent to destroy or steal information.

Types:

- Viruses
- Worms
- Trojan horses
- Active web scripts
- Backdoors
- Spyware

6) What are Distributed Denial-of-service (DDoS) and DoS? (Nov /Dec 2011)

DDoS

- ❖ DDoS is an attack in which a coordinated stream of requests is launched against a target from many locations at the same time.

DoS

- ❖ attacker sends a large number of connection or information requests to a target

- ❖ so many requests are made that the target system cannot handle them successfully along with other, legitimate requests for service
- ❖ may result in a system crash, or merely an inability to perform ordinary functions

7) Distinguish between attack and threat.

Attack	Threat
An act which is in process.	A promise of an attack to come.
An attack is intentional.	Threat can be either intentional or unintentional
Attack to information might have a chance to alter or damage the information when it is successful.	Threat to information does not mean that it is damaged or changed

8) List the counter measures on threats. (NOV/DEC 2012,APRIL/MAY 2015)

To protect an organization's information,

1. **Know yourself**: be familiar with the information to be protected, and the systems that store, transport and process it.

2. Know the threats you face: To make sound decisions about information security, management must be informed about the various threats facing the organization, its application, data and information systems.

9) Why is information security a management problem? What can management do that technology cannot? (NOV/DEC 2011, MAY/JUNE 2014)

- ✓ General management and IT management are responsible for implementing information security to protect the ability of the organization to function.
- ✓ Decision-makers in organizations must set policy and operate their organization in a manner that complies with the complex, shifting political legislation on the use of technology.
- ✓ Management can also implement an effective information security program to protect the integrity and value of the organization's data.

10) What is the difference between criminal law and civil law? (NOV/DEC 2011)

Criminal law	Civil law
Criminal law is the body of law that deals with crime and the legal punishment of criminal offenses.	It deals with the disputes between individuals, organizations, or between the two, in which compensation is awarded to the victim.
To maintain the stability of the state and society by punishing offenders and deterring them and others from	To deal with the disputes between individuals, organizations, or between the two, in which compensation is awarded

offending.	to the victim.

11) **Which law amended the computer Fraud and Abuse act of 1986 and what did it change?(APR 2014)**

LAW: Key U.S Laws of interest to information security professionals

SUBJECT: Threats to computers (1986)

DESCRIPTION: Defines and formalizes laws to counter threats from computer related acts & offenses

12) **What is policy? How it is different from law? (NOV/DEC 2011, MAY/JUNE 2013)**

In an organization is professionals help to maintain security through establishment and enforcement of policies. Thus policy is a body of expectations that describe acceptable and unacceptable employee behaviors in workplace. The main difference between policy and law is that the ignorance of a policy is an acceptable defense.

13) **What are the types of password attacks? What can a systems administrator to do protect against them? (NOV/DEC 2014)**

1. Password crack
2. Brute Force
3. Dictionary

To protect against password attacks, security administrators can:

a. Implement controls that limit the number of attempts allowed.
b. Use a "disallow" list of passwords from a similar dictionary.
c. Require use of additional numbers and special characters in passwords.

PART B

1) **What are the four important functions that the information security performs in an organization? (Nov /Dec 2011, May/June 2015, Nov/Dec 2012)**

Information security performs four important functions in an organization:

- Protects the organization's ability to function
- Enables the safe operation of applications implemented on the organization's IT systems
- Protects the data that the organization collects and uses
- Safeguards the technology assets in use at the organization

1. Protecting the Ability of the Organization to Function

- Both general management and IT management are responsible for implementing information security that protects the ability of the organization to function.
- Decision makers in organizations must
  - Set policy and

- Operate their organization in compliance with the complex,
- Shifting political legislation on the use of technology.

- Although many business and government managers shy away form addressing information security because of its perceived technical complexity, it is important to understand that information security has more to do with management than with technology.
- "In fact," A lot of [Information Security] is good management for information technology.

2. Enabling the Safe Operation of Applications

- Today's organizations are under immense pressure
  - To create and
  - Operate integrated,
  - Efficient, and
  - Capable applications.
- Under this pressure, management is responsible for
  - Informed policy choices and
  - The enforcement of decisions that affect applications and
  - The IT infrastructures that support them.
- The modern organization needs to create an environment that safeguards applications using the organization's IT systems, particularly those elements of the environment that make up the infrastructure of the organization.
- These elements include
  - operating system platforms,
  - electronic mail (e- mail) and
  - Instant Messenger (IM) applications.
- Organizations enable these elements either by subscription from an Internet Service provider (ISP) or by building their own.
- Once the infrastructure is in place, management must understand it has not abdicated to the IT department its responsibility to make **choices and enforce decisions**, but must continue to oversee the infrastructure.

3. Protecting Data that Organizations Collect and use

- Many organization realize that one of their most valuable assets is their data, because without data,
  - An organization loses its record of transactions and / or
  - Its ability to deliver value to its customers.

- Any business, educational institution, or government agency that functions within the modern social context of connected and responsive service relies on information systems to support these services.
- Even if the transaction is not online, information systems and the data they process enable the creation and movement of goods and services.
- The critical aspects of information security

- Protecting data in motion and
- Data at rest

- The significant value of data motivates attackers to steal, sabotage, or corrupt it.
- An effective information security program implemented by management is
  - Essential to the protection of the integrity and
  - Value of the organization's data.

4. Safeguarding Technology Assets in Organizations

- To perform effectively, organizations must add secure infrastructure services based on
  - The size and
  - Scope of the enterprise.

- For instance, a small business may get by with using an e-mail service provided by an ISP, augmented with a personal encryption tool.

- When an organization grows
  - More capabilities are needed
  - Additional security services may have to be provided locally.
- You need to know that PKI involves the use of digital certificates to
  - Ensure the confidentiality of Internet communications &
  - Transactions.

- The PKI offers advanced features such as
  - Efficient key management across and between organizations and
  - Key recovery when keys are loss, likewise,
  - As the organizations network grows to accommodate changing needs

2) Explain various forms of attacks. (May/June 2015, Nov/Dec 2014, Nov/Dec 2012)

- An attack is the deliberate act that **exploits vulnerability**.
- It is accomplished by a threat agent that damages or steals an organization's information or physical asset.
  - An **exploit** is a technique to compromise a system.
  - **Vulnerability** is an identified weakness of a controlled system with controls that are not present or are no longer effective.

In the following headings the various attacks are explained:

Malicious Code

- This kind of 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 in attacking systems in 2002 is the multivector (or polymorphic) worm.

Table Attack Replication Vectors.

Vector	Description
IP scan and attack	Infected system scans 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.**
Web browsing	If the infected system has write access to any Web pages, it makes all Web content files (.html, .asp and others) infectious, so that users who browse to those pages becomes infected.
Virus	Each infested machine infects certain common executable or script files on all computers to which it can write with virus code that can cause infection.
Shares	Using vulnerabilities in file systems and the way many organizations configures them it copies the viral component to all locations it can reach.
Mass mail	By sending e-mail infections to addresses found in the infected system's address book, copies of the infection are sent to many users whose mail-reading programs automatically run the program and infect other systems.
Simple Network Management Protocol (SNMP)	SNMP stands for simple network management protocol. It is a way that servers can share information about their current state, and also a channel through which an administer can modify pre-defined values. While the protocol itself is very simple, the structure of programs that implement SNMP can be very complex. SNMP is a protocol that is implemented on the application layer of the networking stack. There are multiple versions of the SNMP protocol, and many networked hardware devices implement some form of SNMP access. a network being profiled by SNMP will mainly consist of devices containing SNMP agents. An agent is a program that can gather information about a piece of hardware, organize it into predefined entries, and respond to queries using the SNMP protocol.

Hoaxes

- A more devious approach to attacking computer systems is the transmission of a virus hoax, with a real virus attached.
- By masking the attack in a seemingly legitimate message, unsuspecting users more readily distribute it, as they try to do the right thing to avoid infection.
- They send the attack on to their coworkers and friends, infecting many users along the way.
- An attacker can gain access to a system or network resources through a back door. Sometimes these are features left behind by system designers or maintenance staff (as in trap doors)."

Password Crack

- Attempting to reverse calculate a password is often called **cracking.**
- A cracking attack is a component of many dictionary attacks.
- It is used when a copy of the Security Account Manager (SAM) data file can be obtained.
- The SAM file contains the hashed representation of the user's password.
- A password can be hashed using the same algorithm and compared to the hashed results. If they are the same, the password has been guessed.

Brute Force

- The application of computing and network resources to try every possible combination of options of a password is called a **brute force attack**.
- This is often an attempt to repeatedly guess passwords to commonly used accounts; it is sometimes called a **password attack**.
- If attackers can narrow the field of accounts to be attacked, they can devote more time and resources to attacking fewer accounts.

Dictionary attack

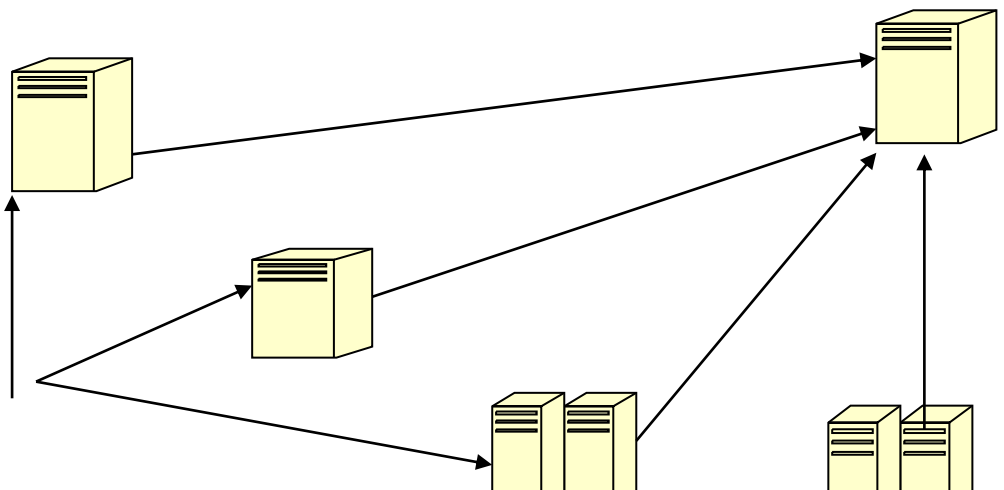
- Narrows the field by selecting specific accounts to attack and uses a list of commonly used passwords (the dictionary) with which to guess, instead of random combinations.
- Organizations that use similar dictionaries to disallow passwords during the reset process guard against easy-to-guess passwords.

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 cannot handle them successfully along with other, legitimate requests for service.
- This may result in a system crash, or merely an inability to perform ordinary functions.

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.
- The compromised machines are turned into zombies, directed towards the target, and executed remotely (usually by a transmitted command) by the attacker.
- DDoS attacks are the most difficult to defend against, and there are presently no controls that any single organization can apply.



ATTACKER

Denial-of-Service Attacks

Spoofing

- Spoofing is a technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host.
- To engage in IP spoofing, a hacker must first use a variety of techniques to find an IP address of a trusted host and then modify the packet headers so that it appears that the packets are coming from that host.
- Newer routers and firewall arrangements can offer protection against IP spoofing.

Data Payload	IP Source 192.160.0.25	IP Destination 100.0.0.75

Data Payload	IP Source 192.160.0.25	IP Destination 100.0.0.75

IP Spoofing

Man-in-the-Middle

- In the well-know man-in-the-middle or TCP hijacking attack,
- An attacker sniffs packets from the network, modifies them, and inserts them back into the network.
- It 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.

In a variant on the TCP hijacking session

- **spoofing** :- involves the interception of an encryption key exchange, where in
- **Main-in-the-middle hacker: -** acts as an invisible middle-man allowing him to eavesdrop on encrypted communications.

Man-in-the-Middle Attack

Spam

- Spam is unsolicited commercial e-mail.
- While many consider spam a nuisance rather than an attack, it is emerging as a vector for some attacks.
- In March 2002, reports emerged of malicious code embedded in MP3 files that were included as attachments to spam.

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 through social engineering or by exploiting various technical flaws in the Simple Mail Transport Protocol.
- This results in the target receiving large volumes of unsolicited e-mail, which they are unable to manage.
- By sending large e-mails with forged header information, poorly configured e-mail systems on the Internet can be tricked into sending many e-mails to an address chosen by the attacker..

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 from a network.
- 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.
- They often work on TCP/IP networks, where they're sometimes called packet sniffers.
- Sniffers add risk to the network, since many systems and users send information on local networks in clear text.
- A sniffer program shows all the data going by, including passwords and the data inside of files, such as word-processing documents and screens full of sensitive data from applications.

Social Engineering

- **Social engineering** is the process of using social skills to convince people to reveal access credentials or other valuable information to the attacker.

This can be done in **several ways**

- Usually involving the perpetrator posing as a person higher in the organizational hierarchy than the victim.

Buffer Overflow

- When the buffer overflows, the attacker can make the target system execute instructions, or the attacker can take advantage of some other unintended consequences of the failure.
- Sometimes this is limited to a denial-of-service,
- The **timing attack** works by

- Exploring the contents of a Web browser's cache
- The attacks allow a Web designer to create a malicious form of cookie to store on the client's system.
- Allow the designer to collect information on access to password protected sites.

3) Discuss the different kinds of threats to an information security. (APRIL/MAY 2015) Explain the various groups of threats faced by an organization. (NOV/DEC 2011) Explain the five groups of threats to information security. (MAY/JUNE 2014)

To investigate the wide range of threats that pervade the interconnected world, researchers have interviewed practicing information security personnel and examined information security literature. While the categorizations may vary, threats are relatively well researched and, consequently, fairly well understood. There is wide agreement that the threat from external sources increases when an organization connects to the Internet.

1. Acts of Human Error or Failure:

Acts performed without intent or malicious purpose by an authorized user. Making of incorrect assumptions. It maintains an entry of erroneous data. Accidental deletion or modification of data is maintained. Storage of data in unprotected areas and failure to protect information. It can be prevented with

- Training
- Ongoing awareness activities
-Verification by a second party
- Many military applications have robust, dual- approval controls built in applications.

2. Compromises to Intellectual Property

It is defined as the ownership of ideas and control over the tangible or virtual representation of those ideas. Intellectual property includes trade secrets, copyrights, trademarks, and patents. Once intellectual property has been defined and properly identified, breaches to IP constitute a threat to the security of this information. Organization purchases or leases the IP of other organizations.

Most Common IP breach is the unlawful use or duplication of software based intellectual property more commonly known as **software Piracy**. Software Piracy affects the world economy. U.S provides approximately 80% of world's software. In addition to the laws surrounding software piracy, two watch dog organizations investigate allegations of software abuse.

1. Software and Information Industry Association (SIIA)
   (i.e.) Software Publishers Association
2. Business Software Alliance (BSA)

Another effort to combat (take action against) piracy is the online registration process.

3. Deliberate Acts of Espionage or Trespass

Deliberate software attacks occur when an individual or group designs and deploys software to attack a system. Most of this software is referred to as malicious code or malicious software, or sometimes malware. These software components or programs are designed to damage, destroy, or deny service to the target systems. Some of the more common instances of malicious code are viruses and worms, Trojan horses, logic bombs, and back doors.

Trespass

It can lead to unauthorized real or virtual actions that enable information gatherers to enter premises or systems they have not been authorized to enter. Sound principles of authentication & authorization can help organizations protect valuable information and systems.

Hackers-> "People who use and create computer software to gain access to information illegally". There are generally two skill levels among hackers.

Expert Hackers-> Masters of several programming languages, networking protocols, and operating systems.

Unskilled Hackers

4. Deliberate Acts of information Extortion (obtain by force or threat)

Possibility of an attacker or trusted insider stealing information from a computer system and demanding compensation for its return or for an agreement not to disclose the information.

5. Deliberate Acts of sabotage or Vandalism

It includes the following:

- Destroy an asset
- Damage the image of organization
- Cyber terrorism-Cyber terrorists hack systems to conduct terrorist activities through network or internet pathways.

6. Deliberate Acts of Theft

Illegal taking of another's property-- is a constant problem. Within an organization, property can be physical, electronic, or intellectual. Physical theft can be controlled by installation of alarm systems. It maintains trained security professionals. It also include the electronic theft control which is under research.

7. Deliberate Software Attacks

Deliberate software attacks occur when an individual or group designs and deploys software to attack a system. Most of this software is referred to as malicious code or malicious software, or sometimes malware. These software components or programs are designed to damage, destroy, or deny service to the target systems. Some of the more common instances of malicious code are viruses and worms, Trojan horses, logic bombs, and back doors.

4) Discuss in detail about virus and worms. (MAY/JUNE 2013)

Virus & Worm Hoaxes

- A computer virus consists of segments of code that perform malicious actions.
- This code behaves very much like a virus pathogen that attacks animals and plants, using the cell's own replication machinery to propagate the attack beyond the initial target.
- The code attaches itself to an existing program and takes control of that program's access to the targeted computer.
- The virus-controlled target program then carries out the virus's plan by replicating itself into additional targeted systems. Many times users unwittingly help viruses get into a system.
- Opening infected e-mail or some other seemingly trivial action can cause anything from random messages popping up on a user's screen to the complete destruction of entire hard drives of data.
- Most organizations block e-mail attachments of certain types and also filter all e-mail for known viruses.
- Now, computers are networked, and e-mail programs prove to be fertile ground for computer viruses unless suitable controls are in place.
- The current software marketplace has several established vendors, such as Symantec Norton Anti-Virus and McAfee Virus scan that provide applications to assist in the control of computer viruses.
- Among the most common types of information system viruses are the macro virus, which is embedded in automatically executing macro code used by word processors, spread sheets, and database applications, and the boot virus, which infects the key operating system files located in a computer's boot sector.

Worm

- A worm is a malicious program that replicates itself constantly, without requiring another program environment.
- Worms can continue replicating themselves until they completely fill available resources, such as memory, hard drive space, and network bandwidth.
- A program or algorithm that replicates itself over a computer network and usually performs malicious actions. The complex behavior of worms can be initiated with or without the user downloading or executing the file.
- Once the worm has infected a computer, it can redistribute itself to all e-mail addresses found on the infected system.

- Furthermore, a worm can deposit copies of itself onto all Web servers that the infected system can reach, so that users who subsequently visit those sites become infected.
- Worms also take advantage of open shares found on the network in which an infected system is located, placing working copies of the worm code onto the server so that users of those shares are likely to become infected.

Trojan horse

- Trojan horses are software programs that hide their true nature and reveal their designed behavior only when activated.
- Trojan horses are frequently disguised as helpful, interesting, or necessary pieces of software, such as readme.exe files often included with shareware or freeware packages.
- A destructive program that masquerade on beginning application, unlike viruses, Trojan horse do not replicate themselves.

Back Door or Trap Door

A virus or worm can have a payload that installs a back door or trap door component in a system, which allows the attacker to access the system at will with special privileges.

Polymorphic Threats

A polymorphic threat is one that over time changes the way it appears to antivirus software programs, making it undetectable by techniques that look for preconfigured signatures. These viruses and worms actually evolve, changing their size and other external file characteristics to elude detection by antivirus software programs.

Virus and Worm Hoaxes

A number of Internet resources enable individuals to research viruses to determine if they are fact or fiction. For the latest information on real, threatening viruses and hoaxes, along with other relevant and current security information, visit the CERT Coordination Center

Blended threat

Blended threats combine the characteristics of virus, worm, Trojan horses & malicious code with server and Internet Vulnerabilities.

Antivirus Program

A Utility that searches a hard disk for viruses and removes any that found.

Forces of Nature

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

Flood: An overflowing of water onto an area that is normally dry, causing direct damage to all or part of the information system or to the building that houses all or part of the information system.

Earthquake: Earthquake: A sudden movement of the earth's crust caused by the release of stress accumulated along geologic faults or by volcanic activity.

Lightning: An abrupt, discontinuous natural electric discharge in the atmosphere. Lightning usually directly damages all or part of the information system or its power distribution components. It can also cause fires or other damage to the building that houses all or part of the information system, and disrupt operations by interfering with access to the buildings that house all or part of the information system.

Landslide/Mudslide: Land- or mudslides also disrupt operations by interfering with access to the buildings that house all or part of the information system. This threat can sometimes be mitigated with casualty insurance and/or business interruption insurance. Since it is not possible to avoid force of nature threats, organizations must implement controls to limit damage

Hurricane or typhoon: A severe tropical cyclone originating in the equatorial regions of the Atlantic Ocean or Caribbean Sea or eastern regions of the Pacific Ocean (typhoon), traveling north, northwest, or northeast from its point of origin, and usually involving heavy rains. These storms can directly damage all or part of the information system or, more likely, the building that houses it.

Tsunami: A very large ocean wave caused by an underwater earthquake or volcanic eruption. These events can directly damage all or part of the information system or, more likely, the building that houses it. Organizations located in coastal areas may experience tsunamis. Tsunamis may also cause disruption to operations through interruptions in access or electrical power to the buildings that house all or part of the information system.

Electrostatic discharge (ESD): Usually, static electricity and ESD is little more than a nuisance. Unfortunately, however, the mild static shock we receive when walking across a carpet can be costly or dangerous when it ignites flammable mixtures and damages costly electronic components. Static electricity can draw dust into clean-room environments or cause products to stick together.

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

5) **Explain the ethical concepts in information security.(NOV/DEC 2011,NOV/DEC 2012)**

Law and ethics in information security

- ✓ The rules with 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.

Policy versus law

The policies guidelines that will describe acceptable and unacceptable employee behaviors in the workplace function as organizational laws complete with penalties, judicial practices, and sanctions to require compliance. Thus, for a policy to become enforceable, it must meet the following five criteria:

Dissemination (distribution): The organization must be able to demonstrate that the relevant policy has been made readily available for review by the employee. Common dissemination techniques include hard copy and electronic distribution.

Review (reading): The organization must be able to demonstrate that it disseminated the document in an intelligible form, including versions for illiterate, non-English reading,and reading-impaired employees. Common techniques include recordings of the policy in English and alternate languages.

Comprehension (understanding): The organization must be able to demonstrate that the employee understood the requirements and content of the policy. Common techniques include quizzes and other assessments.

Compliance (agreement): The organization must be able to demonstrate that the employee agreed to comply with the policy through act or affirmation. Common techniques include logon banners, which require a specific action (mouse click or keystroke) to acknowledge agreement, or a signed document clearly indicating the employee has read, understood, and agreed to comply with the policy.

Uniform enforcement: The organization must be able to demonstrate that the policy has been uniformly enforced, regardless of employee status or assignment.

Types of Laws

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.

Relevant U.S Laws

The implementation of information security legislation contributes to a more reliable business environment, which in turn, enables a stable economy. In its global leadership capacity, the United States has demonstrated a clear understanding of the importance of securing information and has specified penalties for people and organizations that breach U.S. civil statutes.

General computer crime laws

The Computer Fraud and Abuse Act of 1986 (CFA Act) is the cornerstone of many computer-related federal laws and enforcement efforts. The severity of the penalty depends on the value of the information obtained and whether the offense is judged to have been committed:

1. For purposes of commercial advantage
2. For private financial gain
3. Furtherance of a criminal act

Privacy of Customer Information

Privacy of Customer Information Section of the common carrier regulation states that any proprietary information shall be used explicitly for providing services, and not for any marketing purposes, and that carriers cannot disclose this information except when necessary to provide their services. The following agencies, regulated businesses, and individuals are exempt from some of the regulations so that they can perform their duties:

- Bureau of the Census
- National Archives and Records Administration
- Congress
- Comptroller General
- Federal courts with regard to specific issues using appropriate court orders
- Credit reporting agencies
- Individuals or organizations that demonstrate that information is necessary to protect
  the health or safety of that individual

The Security and Freedom through Encryption Act of 1999 provides guidance on the use of encryption and provides protection from government intervention. The acts include provisions that:

DMCA

The DMCA includes the following provisions:

- ✓ It prohibits the circumvention protections and counter measures implemented by copyright owners to control access to protected content.
- ✓ Prohibits the manufacture of devices to circumvent protections and countermeasures that control access to protected content.
- ✓ Bans trafficking in devices manufactured to circumvent protections and countermeasures that control access to protected content Prohibits the altering of information attached or imbedded into copyrighted material.

- ✓ Excludes Internet service providers from certain forms of contributory copyright infringement.

Differing unethical and illegal behavior

There are three general causes of unethical and illegal behavior:

Ignorance

Ignorance of the law is no excuse; however, ignorance of policy and procedures is. The first method of deterrence is education. This is accomplished by means of designing, publishing, and disseminating organization policies and relevant laws, and also obtaining agreement to comply with these policies and laws from all members of the organization. Reminders, training, and awareness programs keep the policy information in front of the individual and thus better support retention and compliance.

Accident

Individuals with authorization and privileges to manage information within the organization are most likely to cause harm or damage by accident. Careful planning and control helps prevent accidental modification to systems and data.

Intent

Criminal or unethical intent goes to the state of mind of the person performing the act; it is often necessary to establish criminal intent to successfully prosecute offenders. Protecting a system against those with intent to cause harm or damage is best accomplished by means of technical controls, and vigorous litigation or prosecution if these controls fail.

Spoofing

It is a technique used to gain unauthorized access to computers, where in the intruder sends messages to a computer that has an IP address that indicates that the messages are coming from a trusted host.

Legal, Ethical and Professional Issues in Information Security

- ✓ The information security professional plays an important role in an organization's approach to managing liability for privacy and security risks.
- ✓ In the modern litigious societies of the world, sometimes laws are enforced in civil courts, where large damages can be awarded to plaintiffs who bring suits against organizations.
- ✓ The Law and Ethics in Information Security. **Laws** are rules that mandate or prohibit certain behavior in society; they are drawn from **ethics**, which define socially acceptable behaviors. The key difference between laws and ethics is that laws carry the sanctions of a governing authority and ethics do not.
- ✓ Ethics in turn are based on **Cultural mores.** Ethics define socially acceptable behaviors. Ethics in turn are based on cultural mores. Fixed moral attitudes or customs of a particular group. The Security and Freedom through Encryption Act of 1999 provides

guidance on the use of encryption and provides protection from government intervention. The acts include provisions that:

- Reinforce an individual's right to use or sell encryption algorithms, without concern for regulations requiring some form of key registration. Key registration is the storage of a cryptographic key (or its text equivalent) with another party to be used to break the encryption of data. This is often called "key escrow."
- Prohibit the federal government from requiring the use of encryption for contracts, grants, and other official documents and correspondence.
- The use of encryption is not probable cause to suspect criminal activity.
- Relax export restrictions by amending the Export Administration Act of 1979.
- Provide additional penalties for the use of encryption in the commission of a criminal act.

The **Freedom of Information Act** allows any person to request access to federal agency records or information not determined to be a matter of national security. Agencies of the federal government are required to disclose any requested information on receipt of a written request. This requirement is enforceable in court. Some information is, however, protected from disclosure, and the act does not apply to state or local government agencies or to private businesses or individuals, although many states have their own version of the FOIA.

UNIT III

SECURITY ANALYSIS

Risk Management: Identifying and Assessing Risk, Assessing and Controlling Risk

PART A

1. What is risk management? (Nov /Dec 2011, Nov/Dec 2012)

Risk management is the process of identifying vulnerabilities in an organization's information systems and taking carefully reasoned steps to assure

- Confidentiality
- Integrity
- Availability

2. **In risk management strategies, why does a periodic review have to be a part of process? (May/June 2012, May/June 2013)**
   - The first focus is asset inventory
   - The completeness and accuracy of the asset inventory has to be verified
   - The threats and vulnerabilities that are dangerous to asset inventory must be verified.
   - It is a constant process for safeguards and controls to be devised and implemented, and not to be installed and forget devices.
3. **What is Vulnerability Identification? (May/June 2015, Nov/Dec 2014)**
   - Vulnerabilities are specific avenues that threat agents can exploit to attack an information asset
   - Examine how each of the threats that are possible or likely could be perpetrated and list the organization's assets and their vulnerabilities
   - The process works best when groups of people with diverse backgrounds within the organization work iteratively in a series of brainstorming sessions
4. **What is asset valuation? List the components of asset valuation. (May/June 2012)**

   A method of assessing the worth of a company, real property, security, antique or other item of worth. Asset valuation is commonly performed prior to the sale of an asset or prior to purchasing insurance for an asset.

   <u>Components:</u>

   - People
   - Procedure
   - Data and information
   - Software
   - Hardware
   - Network Elements
5. **What are the different types of Access Controls?**
   - Discretionary Access Controls (DAC)
   - Mandatory Access Controls (MACs)
   - Nondiscretionary Controls
   - Role-Based Controls
   - Task-Based Controls
   - Lattice-based Control

6. **What is the goal of documenting results of the risk assessment?**
    - The goal is to identify the information assets of the organization that have specific vulnerabilities and create a list of them, ranked for focus on those most needing protection first
    - In preparing this list, we have collected and preserved factual information about the assets, the threats they face, and the vulnerabilities they experience
7. **What is the formula for calculating risk?**

> Risk = Threat x Vulnerability x Cost
>
> Risk Assessment = ((Likelihood + Impact + Current Impact)/3) * 2 - 1

8. **Define Disaster Recovery Plan (May/June 2014)**

    The most common mitigation procedure is Disaster Recovery Plan (DRP). The DRP includes the entire spectrum of activities used to recover from the incident and strategies to limit losses before and after the disaster. DRP usually include all preparations for the recovery process, strategies to limit losses during the disaster.

9. **What is the difference between benchmark and baseline? (NOV/DEC 2011)**

Benchmark	Baseline
An alternative approach to risk management	Base line is the analysis of measures against established standards
The process of seeking out and studying the practices used in other organizations that produce results you would like to duplicate in your organization	In information security, baselining is comparing security activities and events against the organization's future performance.

10. **Why do networking components need more examination from IS perspective than from System development perspective? (MAY/JUNE 2014)**

Networking components need more examination from an information security perspective than from a systems development perspective because networking subsystems are often the focal point of attacks against the system and they should be considered as special as cases rather than combined

11. **What is cost benefit analysis? (NOV/DEC 2014)**

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. The formal process to document this decision making process is called a cost benefit analysis or an economic feasibility study.

12. **What is risk mitigation? (APRIL/MAY 2015)**

The process by which an organization introduces specific measures to minimize or eliminate unacceptable *risks* associated with its operations. *Risk mitigation* measures can be directed towards reducing the severity of *risk* consequences, reducing the probability of the *risk*

13. Give the meaning of dumpster diving with respect to information security? (MAY/JUNE 2013)

Dumpster diving dumpster diving is a technique used to retrieve information that could be used to carry out an attack on a computer network. Dumpster diving limited to searching through the trash for obvious treasures like access codes or passwords is included in the management of classified data. To retrieve information that could embarrass a company or compromise information security.

14. What is the thumb rules applied in selecting the preferred risk mitigation strategy? (NOV/DEC2012)

The thumb Rules applied in selecting the risk mitigation strategy are as follows:

1. When vulnerability (flaw or weakness) exists: Implement security controls to reduce the likelihood of a vulnerability being exercised.

2. When vulnerability can be exploited, apply layered protections, architectural designs, and administrative controls to minimize the risk.

3. When the attacker's cost is less than his potential gain: Apply protections to increase the attacker's cost.

PART B

1) Explain the asset identification and valuation and its different categories. (Nov/Dec 2012)

Asset Identification and Valuation

- This iterative process begins with the identification of assets, including all of the elements of an organization's system: people, procedures, data and information, software, hardware, and networking elements
- Then, we classify and categorize the assets adding details as we dig deeper into the analysis
- **People, Procedures, and Data Asset Identification**
- Unlike the tangible hardware and software elements already described, the human resources, documentation, and data information assets are not as readily discovered and documented
- These assets should be identified, described, and evaluated by people using knowledge, experience, and judgment
- As these elements are identified, they should also be recorded into some reliable data handling process

Asset Information for People

- Position name/number/ID – try to avoid names and stick to identifying positions, roles, or functions
- Supervisor
- Security clearance level

- Special skills

Categorizing the Components of an Information System

Traditional system components	SecSDLC and 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

Hardware, Software, and Network Asset Identification

- What attributes of each of these information assets should be tracked?
- When deciding which information assets to track, consider including these asset attributes:
  - Name
  - IP address
  - MAC address
  - Element type
  - Serial number
  - Manufacturer name
  - Manufacturer's model number or part number
  - Software version, update revision, or FCO number
  - Physical location
  - Logical location
  - Controlling entity

Asset Information for Procedures

- For Procedures:
  - Description
  - Intended purpose
  - What elements is it tied to
  - Where is it stored for reference
  - Where is it stored for update purposes

Asset Information for Data

- For Data:

- Classification
- Owner/creator/manager
- Size of data structure
- Data structure used – sequential, relational
- Online or offline
- Where located
- Backup procedures employed

2) How information assets are classified? Explain the process of Information asset valuation.

Information Asset Classification

- Many organizations already have a classification scheme
- Examples of these kinds of classifications are:
  - confidential data
  - internal data
  - public data
- Informal organizations may have to organize themselves to create a useable data classification model
- The other side of the data classification scheme is the personnel security clearance structure
  - ***Information Asset Valuation***
- Each asset is categorized
- Questions to assist in developing the criteria to be used for asset valuation:
  - Which information asset is the most critical to the success of the organization?
    - Which information asset generates the **most revenue**?
    - Which information asset generates the **most profitability**?
    - Which information asset would be the **most expensive to replace**?
    - Which information asset would be the **most expensive to protect**?
    - Which information asset would be the most embarrassing or **cause the greatest liability if revealed?**

Information Asset Valuation

- Create a weighting for each category based on the answers to the previous questions
  - Which factor is the most important to the organization?
- Once each question has been weighted, calculating the importance of each asset is straightforward

- List the assets in order of importance using a weighted factor analysis worksheet

System Name: SLS E-Commerce
Date Evaluated: February 2003
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

Example Worksheet for the Asset Identification of Information Systems

TAB ample of a Weighted Factor Analysis Worksheet

Information asset	Criteria 1: impact to revenue	Criteria 2: impact to profitability	Criteria 3: public image impact	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

Notes: EDI: Electronic Data Interchange
SSL: Secure Sockets Layer

3) **Explain the different risk control strategies. Also, explain briefly the plans adopted for mitigation of risks. (Nov /Dec 2011, May/June 2015, Nov/Dec 2014, Nov/Dec 2012)**

Four basic strategies are used to control the risks that result from vulnerabilities:

- Apply safeguards **(avoidance**)
- Transfer the risk (**transference**)
- Reduce the impact (**mitigation**)
- Inform themselves of all of the consequences and accept the risk without control or mitigation (**acceptance**)

Risk Control Strategies: Avoidance

- **Avoidance** attempts to prevent the exploitation of the vulnerability
- This is the preferred approach, as it seeks to avoid risk in its entirety rather than dealing with it after it has been realized
- Accomplished through countering threats
  - removing vulnerabilities in assets
  - limiting access to assets
  - adding protective safeguards
- Three areas of control:
  - Policy
  - Training and education
  - Technology

Transference

Transference is the control approach that attempts to shift the risk to other assets, other processes, or other organizations

- If an organization does not already have quality security management and administration experience, it should hire individuals or firms that provide such expertise
- This allows the organization to transfer the risk associated with the management of these complex systems to another organization with established experience in dealing with those risks

Mitigation

- **Mitigation** attempts to reduce the impact of exploitation through planning and preparation
- Three types of plans:
  - **disaster recovery planning (DRP)**
    - The most common of the mitigation procedures is the disaster recovery plan or DRP
  - **business continuity planning (BCP)**
    - Longer term issues are handled in the business continuity plan or BCP
  - **incident response planning (IRP)**

- The actions to take while the incident is in progress are defined in the incident response plan or IRP

❖ ***Acceptance***

- **Acceptance** of risk is doing nothing to close a vulnerability and to accept the outcome of its exploitation
- Acceptance is valid only when:
  - Determined the level of risk
  - Assessed the probability of attack
  - Estimated the potential damage
  - Performed a thorough cost benefit analysis
  - Evaluated controls using each appropriate feasibility
  - Decided that the particular function, service, information, or asset did not justify the cost of protection
- Risk appetite describes the degree to which an organization is willing to accept risk as a trade-off to the expense of applying controls

a) Incidence Response Plan

The actions an organization can perhaps should take while the incident is in progress are documented in what is known as Incident Response Plan (IRP)

IRP provides answers to questions victims might pose in the midst of the incident, such as "What do I do now?"

Answers to the following type of questions will be provided in IRP:

a. What should the administrator should do first?
b. Whom should they contact?
c. What should they document?

For example, in the event of serious virus or worm outbreak, the IRP may be used to assess the likelihood of imminent damage and to inform key decision makers in the various communities of interest.

b) Disaster Recovery Plan

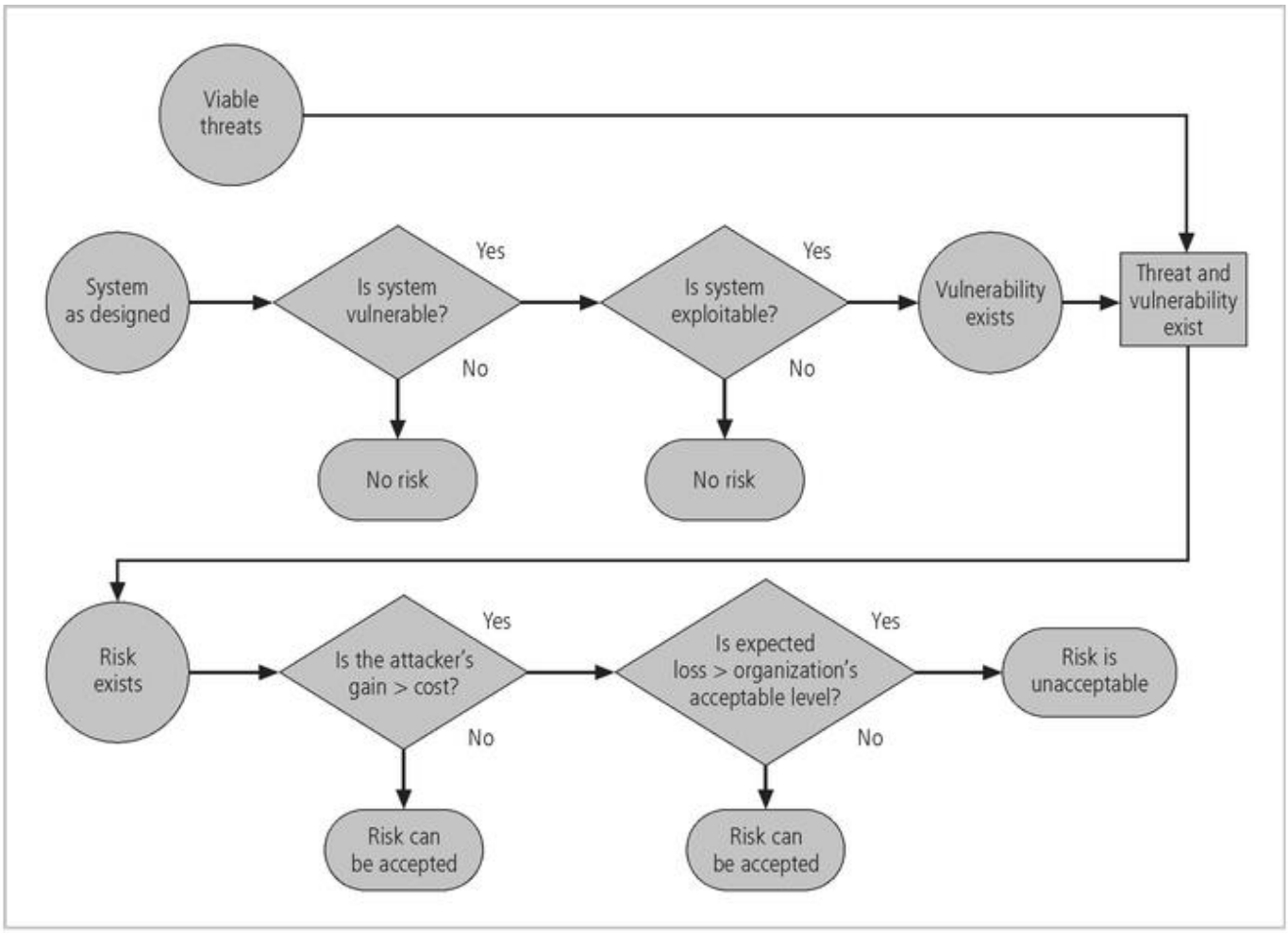
The most common mitigation procedure is Disaster Recovery Plan (DRP). The DRP includes the entire spectrum of activities used to recover from the incident. DRP can include strategies to limit losses before and after the disaster. These strategies are fully deployed once the disaster has stopped.

DRP usually include all preparations for the recovery process, strategies to limit losses during the disaster, and detailed steps to follow when the smoke clears, the dust settles, or the floodwaters recede.

c) Business Continuity Plan

The BCP is the most strategic and long term of the three plans. It encompasses the continuation of business activities if a catastrophic event occurs, such as the loss of an entire database, building or entire operations center. The BCP includes the planning the steps necessary to ensure the continuation of the organization when the scope or scale of a disaster exceeds the ability of the DRP to restore operations. This can include

preparation steps for activation of secondary data centers, hot sites, or business recovery sites.



Risk Handling Decision Points[7]

4) Describe the process of risk identification in detail. (NOV/DEC 2011, NOV/DEC 2012)

Sketch and explain the components of risk identification process. (MAY/JUNE 2013)

Risk Identification

Risk identification is the process of examining and documenting the security posture of an organization's information technology and the risk it faces. IT professionals know their organization's information assets through identifying, classifying and prioritizing them. Assets are the targets of various threats and threat agents, and the goal is to protect the assets from the threats.

The process of Risk Identification begins with the identification of the organization's information assets and an assessment of their value.

Asset Identification & Valuation

It includes all the elements of an organization's system, such as people, procedures, data and information, software, hardware, and networking elements.

Then classify and categorize the assets, adding details. People include employees and nonemployees. There are two categories of employees: those who hold trusted roles and have correspondingly greater authority and accountability, and other staff who have assignments without special privileges.

Data Components have been expanded to account for the management of information in all stages:

1. Transmission
2. Processing
3. Storage

- **Software Components** can be assigned to one of three categories: Applications, Operating Systems, or security components.
- **Hardware** is assigned to one of two categories: the usual systems devices and their peripherals, and the devices that are part of information security control systems. The latter must be protected more thoroughly than the former.

People, Procedures & Data Asset Identification

People : Position name/number/ID: Supervisor; Security clearance level; special skills.

Procedures: Description/intended purpose/relationship to software / hardware and networking elements; storage location for update; storage location for reference.

Data: Classification; owner; Creator; Manager; Size of data structure; data structure used; online/offline/location/backup procedures employed.

Hardware, Software, and Network Asset Identification

It depends on the needs of the organization and its risk management efforts.

Name: Should adopt naming standards that do not convey information to potential system attackers.

IP address: Useful for network devices & Servers. Many organizations use the dynamic host control protocol (DHCP) within TCP/IP that reassigns IP numbers to devices as needed, making the use of IP numbers as part of the asset identification process problematic. IP address use in inventory is usually limited to those devices that use static IP addresses.

Media Access Control (MAC) address: Electronic serial numbers or hardware addresses. All network interface hardware devices have a unique number. The MAC address number is used by the network operating system as a means to identify a specific network device. It is used by the client's network software to recognize traffic that it must process.

Element Type: Document the function of each Element by listing its type. For hardware, a list of possible element types, such as servers, desktops, networking devices or test equipment. One server might be listed as:

1. Device class= S (Server)
2. Device OS= W2K (Windows 2000)
3. Device Capacity = AS (Advanced Server)

Serial Number: For hardware devices, the serial number can uniquely identify a specific device.

Manufacturer Name: Record the manufacturer of the device or software component. This can be useful when responding to incidents that involve these devices or when certain manufacturers announce specific vulnerabilities.

Manufacturer's Model No or Part No: Record the model or part number of the element. This record of exactly what the element is can be very useful in later analysis of vulnerabilities, because some vulnerability instances only apply to specific models of certain devices and software components.

Software Version, Update revision, or FCO number: Document the specific software or firmware revision number and, for hardware devices, the current field change order (FCO) number.

Physical location: Note where this element is located physically (Hardware)

Logical Location: Note where this element can be found on the organization's network. The logical location is most useful for networking devices and indicates the logical network where the device is connected.

Controlling Entity: Identify which organizational unit controls the element.

Information Asset Classification- In addition to the categories, it is advisable to add another dimension to represent the sensitivity & Security priority of the data and the devices that store, transmit & process the data.

Information Asset Valuation

As each asset is assigned to its category, posing a number of questions assists in developing the weighting criteria to be used for information asset valuation or impact evaluation.

Security Clearances

The other side of the data classification scheme is the personnel security clearance structure. Each user of data must be assigned a single authorization level that indicates the level of classification he or she is authorized to view.

Management of classified data

It includes its storage, distribution, portability, and destruction. Military uses color coordinated cover sheets to protect classified information from the casual observer. Each classified document should contain the appropriate designation at the top and bottom of each page clean desk policy requires that employees secure all information in appropriate storage containers at the end of each day.

When Information are no longer valuable, proper care should be taken to destroy them by means of shredding, burning or transferring to a service offering authorized document destruction. Dumpster diving is to retrieve information that could embarrass a company or compromise information security.

Vulnerability Identification

- Create a list of Vulnerabilities for each information asset.
- Groups of people work iteratively in a series of sessions give best result.

- At the end of identification process, you have a list of assets and their vulnerabilities.

5) Explain the process of risk assessment and documenting the result of risk assessment. (MAY/JUNE 2014) Discuss the risk assessment in detail. (APRIL/MAY 2015)

Risk Assessment

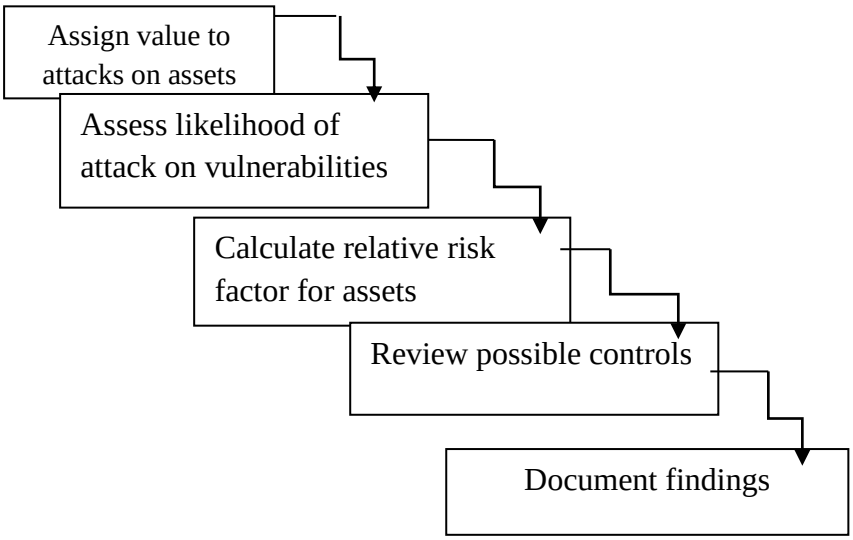
It assigns a risk rating or score to each Information asset. It is useful in gauging the relative risk to each vulnerable asset. Risk is the likelihood of the occurrence of a vulnerability multiplied by the value of the information asset minus the percentage of risk mitigated by current controls plus the uncertainty of current knowledge of the vulnerability.

Major stages of risk assessment

Valuation of Information assets

It assigns weighted scores for the value to the organization of each information asset. National Institute of Standards & Technology (NIST) gives some standards. To be effective, the values must be assigned by asking the following questions.

- Which threats present a danger to an organization's assets in the given environment?
- Which threats represent the most danger to the organization's Information?
- How much would it cost to recover from a successful attack?
- Which of the threats would require the greatest expenditure to prevent?



Likelihood

It is the probability of specific vulnerability within an organization will be successfully attacked. NIST gives some standards.

- 0.1 = Low
- 1.0 = High

Eg: Number of network attacks can be forecast based on how many network address the organization has assigned.

Risk Determination

Risk = Likelihood of vulnerability occurrence) X (Value of information Asset) __ (% of risk mitigated by current controls) + uncertainty of current knowledge of the vulnerability.

- 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

Eg: Information Asset A has a value score of 50 & has one vulnerability: Vulnerability 1 has a likelihood of 1.0 with no current controls, estimate that assumptions and data are 90% accurate.

Solution:

Risk = [(1.0) x 50] – 0% + 10%

= (50 x 1.0) – ((50 x 1.0)x 0.0) + ((50 x 1.0) x 0.1)

= 50 – 0 + 5

= 55

Identify Possible Controls (For Residual Risk)

The residual risk is the risk that remains to the information asset even after the existing control has been applied. The three general categories of controls are as follows:

1. Policies
2. Programs
3. Technologies

1. Policies
   - General Security Policy
   - Program Security Policy
   - Issue Specific Policy
   - Systems Specific Policy
2. Programs
   - Education
   - Training
   - Awareness
3. Security Technologies
   - Technical Implementation Policies

Access Controls

It specially addresses admission of a user into a trusted area of the organization.Eg: Computer rooms, power Rooms. It maintains the combination of policies, programs and technologies

Types of Access controls

Mandatory Access Controls (MACs)

Give users and data owner's limited control over access to information resources.

Nondiscretionary Controls

It is managed by a central authority in the organization; can be based on individual's role (role-based controls) or a specified set of assigned tasks (task-based controls)

Discretionary Access Controls (DAC)

It is implemented at discretion or option of the data user

Lattice-based Access Control

The variation of MAC shows that the users are assigned matrix of authorizations for particular areas of access.

Documenting the Results of Risk Assessment

By the end of the Risk Assessment process, you probably have a collection of long lists of information assets with data about each of them. The goal of this process is to identify the information assets that have specific vulnerabilities and list them, ranked according to those most needing protection. It 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 in the following table.

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)SSL-Secure Sockets Layer	100	Lost orders due to Web server software failure	0.01	1

6) Explain in detail about CBA and benchmarking with its metrics based measures.

(MAY/JUNE 2014)

Cost Benefit Analysis (CBA)

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. The formal process to document this decision making process is called a Cost Benefit analysis or an economic feasibility study.

Cost Benefit Analysis or an Economic Feasibility study

Some of the items that affect the cost of a control or safeguard include:

1. Cost of development or acquisition [purchase cost] of hardware, software and services.
2. Training Fees(cost to train personnel)
3. Cost of Implementation[Cost to install, Configure, and test hardware, software and services]
4. service Costs[Vendor fees for maintenance and upgrades]
5. Cost of maintenance[Labor expense to verify and continually test, maintain and update]

Benefit is the value that an organization realizes by using controls to prevent losses associated with a specific vulnerability.

Amount of benefit = Value of the Information asset and Value at risk.

Asset Valuation is the process of assigning financial value or worth to each information asset.

Some of the components of asset valuation include:

1. Value retained from the cost of creating the information asset.
2. Value retained from past maintenance of the information asset.
3. Value implied by the cost of replacing the information.
4. Value from providing the information.
5. Value incurred from the cost of protecting the information.
6. Value to owners.
7. Value of intellectual property.
8. Value to adversaries.
9. Loss of Productivity while the information assets are unavoidable.
10. Loss of revenue while information assets are unavailable.

The organization must be able to place a dollar value on each collection of information and the information assets it owns. This value is based on the answers to these questions:

- How much did it cost to create or acquire this information?
- How much would it cost to recreate or recover this information?
- How much does it cost to maintain this information?
- How much is this information worth to the organization?
- How much is this information worth to the competition?

A Single loss expectancy (SLE) is the calculation of the value associated with the most likely loss from an attack. It is a calculation based on the value of the asset and the **exposure factor (EF),** which is the expected percentage of loss that would occur from a particular attack, as follows:

Single Loss Expectancy (SLE) = Asset value x Exposure factor [EF]

EF → Expected percentage of loss that would occur from a particular attack.

The probability of threat occurring is usually a loosely derived table indicating the probability of an attack from each threat type within a given time frame (for example, once every 10 years). This value is commonly referred to as the **annualized rate of occurrence (ARO)**

The expected value of a loss can be stated in the following equation:

Annualized loss Expectancy (ALE) which is calculated from the ARO and SLE.

ALE = SLE x ARO

Cost Benefit Analysis (CBA) Formula

CBA is whether or not the control alternative being evaluated is worth the associated cost incurred to control the specific vulnerability. The CBA is most easily calculated using the ALE from earlier assessments before the implementation of the proposed control, which is known as ALE (prior). Subtract the revised ALE, estimated based on control being in place, known as ALE (post). Complete the calculation by subtracting the annualized cost of the safeguard (ACS).

CBA = ALE (Prior) - ALE (Post) - ACS

Where

ALE prior is the Annualized Loss Expectancy of the risk before the implementation of the control.

ALE post is the ALE examined after the control has been in place for a period of time.

ACS is the Annual Cost of the Safeguard.

Bench Marking

An alternative approach to risk management. The process of seeking out and studying the practices used in other organizations that produce results you would like to duplicate in your organization.

One of two measures typically used to compare practices:

- **Metrics-based measures**
- **Process-based measures**

It is good for potential legal protection. Metrics based measures are comparisons based on numerical standards, such as:

1. Numbers of successful attacks.
2. Staff-hours spent on systems protection.
3. Dollars spent on protection.
4. Numbers of Security Personnel.
5. Estimated value in dollars of the information lost in successful attacks.
6. Loss in productivity hours associated with successful attacks.

The difference between an organization's measures and those of others is often referred to as a performance gap. The other measures commonly used in benchmarking are process-based measures. **Process-based measures** are generally less focused on numbers and more strategic than metrics-based-measures.

Due Care/Due Diligence

When organizations adopt levels of security for a legal defense, they may need to show that they have done what any prudent organization would do in similar circumstances - this is referred to as a standard of due care. Due diligence is the demonstration that the organization is diligent in ensuring that the implemented standards continue to provide the required level of protection. The failure to support a standard of due care or due diligence can open an organization to legal liability.

Best Business Practices

The security efforts that provide a superior level of protection of information are referred to as best business practices. The best security practices (BSPs) are security efforts that are among the best in the industry. When considering best practices for adoption in your organization, consider the following:

- Does your organization resemble the identified target?
- Are the resources you can expend similar?
- Are you in a similar threat environment?

Microsoft's Ten Immutable Laws of Security

1. If a bad guy can persuade you to run his program on your computer, it's not your computer anymore
2. If a bad guy can alter the operating system on your computer, it's not your computer anymore
3. If a bad guy has unrestricted physical access to your computer, it's not your computer anymore
4. If you allow a bad guy to upload programs to your web site, it's not your web site anymore

5. Weak passwords trump strong security
6. A machine is only as secure as the administrator is trustworthy
7. Encrypted data is only as secure as the decryption key
8. An out of date virus scanner is only marginally better than no virus scanner at all
9. Absolute anonymity isn't practical, in real life or on the web
10. Technology is not a panacea

Problems

The biggest problem with benchmarking in information security is that organizations don't talk to each other. Another problem with benchmarking is that no two organizations are identical A third problem is that best practices are a moving target.

7) Explain the other feasibility studies considered for a project of IS and briefly explain the data classification and management process. (DEC 2011, JUNE 2013)

Organizational Feasibility

The organizational Feasibility examines how well the proposed information security alternatives will contribute to the efficiency, effectiveness, and overall operation of an organization. The above and beyond the impact on the bottom line, the organization must determine how the proposed alternatives contribute to the business objectives of the organization.

Operational feasibility

Operational feasibility analysis addresses several key areas not covered in the other feasibility measures. 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. One of the fundamental requirements of systems development is user buy-in. If the users do not accept a new technology, policy, or program, it will fail. Users may not openly oppose a change, but if they do not support a control, they will find ways of disabling or circumventing it, thereby creating vulnerability.

Technical Feasibility

In addition to the economic costs and benefits of proposed controls, the project team must also consider the technical feasibilities of their design, implementation, and management. Some safeguards, especially technology-based safeguards, are extremely difficult to implement, configure, and manage. Technical feasibility analysis examines whether or not the organization has or can acquire the technology necessary to implement and support the proposed control.

Political feasibility

For some organizations, the most important feasibility evaluated may be political. Politics has been defined as the art of the possible 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.

In some cases, resources are provided directly to the information security community under a budget apportionment model. The management and professionals involved in information security then allocate the resources to activities and projects using processes of their own design. Another methodology for budget allocation requires the information security team to propose and justify use of the resources for activities and projects in the context of the entire organization. This requires that arguments for information security spending articulate the benefit of the expense for the whole organization, so that members of the organizational communities of interest can understand its value.

Data Classification

1. Confidential
2. Internal
3. External

Confidential: Access to information with this classification is strictly on a need-to-know basis or as required by the terms of a contract.

Internal: Used for all internal information that does not meet the criteria for the confidential category and is to be viewed only by authorized contractors, and other third parties.

External: All information that has been approved by management for public release.

The military uses five level classifications

1. Unclassified data
2. Sensitive But Unclassified data (SBU)
3. Confidential data
4. Secret data
5. Top Secret data

Unclassified data: Information that can generally be distributed to the public without any threat to U.S. National interests.

Sensitive But Unclassified data (SBU) : Any information of which the loss, misuse, or unauthorized access to, or modification of might adversely affect U.S. national interests, the conduct of Department of Defense(DoD) programs, or the privacy of DoD personnel.

Confidential data: Any information or material the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.

Secret: Any information or material the unauthorized disclosure of which reasonably could be cause serious damage to the national security.

Top Secret Data: Any information or material the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.

The organization may have

1. Research data
2. Personnel data
3. Customer data
4. General Internal Communications

Some organization may use

1. Public data
2. For office use only
3. Sensitive data
4. Classified data

Public: Information for general public dissemination, such as an advertisement or public release.

For Official Use Only: Information that is not particularly sensitive, but not for public release, such as internal communications.

Sensitive: Information important to the business that could embarrass the company or cause loss of market share if revealed.

Classified: Information of the utmost secrecy to the organization, disclosure of which could severely impact the well-being of the organization.

Security Clearances

The other side of the data classification scheme is the personnel security clearance structure. Each user of data must be assigned a single authorization level that indicates the level of classification he or she is authorized to view.

Eg: Data entry clerk, development Programmer, Information Security Analyst, or even CIO.

Most organizations have a set of roles and the accompanying security clearances associated with each role. Overriding an employee's security clearance is the fundamental principle of "need-to-know".

Management of classified data

It includes the storage, distribution, portability, and destruction.The military uses color coordinated cover sheets to protect classified information from the casual observer. Each classified document should contain the appropriate designation at the top and bottom of each page.

Dumpster diving: To retrieve information that could embarrass a company or compromise information security.

Threat Identification

After identifying the information assets, the analysis phase moves on to an examination of the threats facing the organization

Vulnerability Identification:

- Create a list of Vulnerabilities for each information asset.
- Groups of people work iteratively in a series of sessions give best result.

- At the end of Identification process, you have a list of assets and their vulnerabilities.

UNIT IV

PART A

1. What is information security policy? (Nov /Dec 2011)

Information security policy is a set of policies issued by an organization to ensure that all information technology users within the domain of the organization or its network comply with rules and guidelines related to the security of the information stored digitally at any point in the network or within the organization's boundaries of authority

2. What are the three types of security policies? (Nov/Dec 2012)

Management defines three types of security policy:

- General or security program policy
- Issue-specific security policies
- Systems-specific security policies

3. What are ACL Policies? (May/June 2015)

ACLs allow configuration to restrict access from anyone and anywhere

ACLs regulate:

- Who can use the system
- What authorized users can access
- When authorized users can access the system
- Where authorized users can access the system from
- How authorized users can access the system

4.What measurement do you use when preparing a potential damage assessment? May/June 2012)

Identify what must be done to recover from each possible case. The costs include the actions of the response team(s) as they act to recover quickly and effectively from an incident or disaster.

5.Mention the Drawbacks of ISO 17799/BS 7799 (Nov /Dec 2011, Nov/Dec 2014)

Several countries have not adopted 17799 claiming there are fundamental problems:

- The global information security community has not defined any justification for a code of practice as identified in the ISO/IEC 17799
- 17799 lack "the necessary measurement precision of a technical standard".
- There is no reason to believe that 17799 is more useful than any other approach currently available
- 17799 is not as complete as other frameworks available
- 17799 is perceived to have been hurriedly prepared given the tremendous impact its adoption could have on industry information security controls
- There is no reason to believe that 17799 is more useful than any other

approach currently available

- 17799 is not as complete as other frameworks available
- 17799 is perceived to have been hurriedly prepared given the tremendous impact its adoption could have on industry information security controls

6. Define policy and standards.(May/June 2012)

A policy is a plan or course of action, as of a government, political party, or business, intended to influence and determine decisions, actions, and other matters. Standards, on the other hand, are more detailed statements of what must be done to comply with policy. The organizational rules for acceptable/unacceptable behavior.

- Penalties for violations
- Appeals process

7.What is contingency planning?(Nov/Dec 2012)

It is the entire planning conducted by the organization to prepare for, react to, and recover from events that threaten the security of information and information assets in the organization. Organizations need to develop disaster recovery plans, incident response plans, and business continuity plans as subsets of an overall CP.

8.What are the resources available in web to assist an organization in developing best practices as part of security framework? (MAY/JUNE 2014)

Web resources that can assist in identifying risk limits and the categorization of web applications into risk pools are considered best practices when creating a security framework. Other steps that a business should take include the generation of risk reports and a database that tracks applications being used and its risk factors.

9.Give any 5 major sections of ISO/IEC 17799 standards. (May/June 2013)

- Organizational Security Policy
- Organizational Security Infrastructure
- Asset Classification and Control
- Personnel Security
- Compliance

10.What are the key technological components used for security implementation?

- A firewall is a device that selectively discriminates against information flowing into or out of the organization
- **DMZ** : A buffer against outside attack is referred to as demilitarized zone. It is a no-man's-land between the inside and outside networks where some organizations place Web Servers.

The servers provide access to organizational Web pages without allowing Web requests to enter the interior networks.

- In an effort to detect unauthorized activity within the inner network, or on individual machines, an organization may wish to implement Intrusion Detection Systems or IDS

11. What is firewall? How does it differ from gateway? (NOV/DEC 2104)

Firewall is a device that selectively discriminates against information flowing into or out of the organization. A Firewall can be a single device or a firewall subnet, which consists of multiple firewalls creating a buffer between the outside and inside networks. Firewalls are usually placed on the security perimeter, just behind or as part of a gateway router.

12. What is an after action review? When it is performed and how it is done? (JUNE 2014)

An after action review (AAR) is a structured review or de modified process for analyzing what happened, why it happened, and how it can be done better by the participants and those responsible for the project or event. An AAR occurs within a cycle of establishing the leader's intent, planning, preparation, action and review. An AAR is distinct from a de-brief in that it begins with a clear comparison of intended vs. actual results achieved.

13. What are the stages in the Business Impact Analysis?

The stages in the business impact analysis step are as follows:

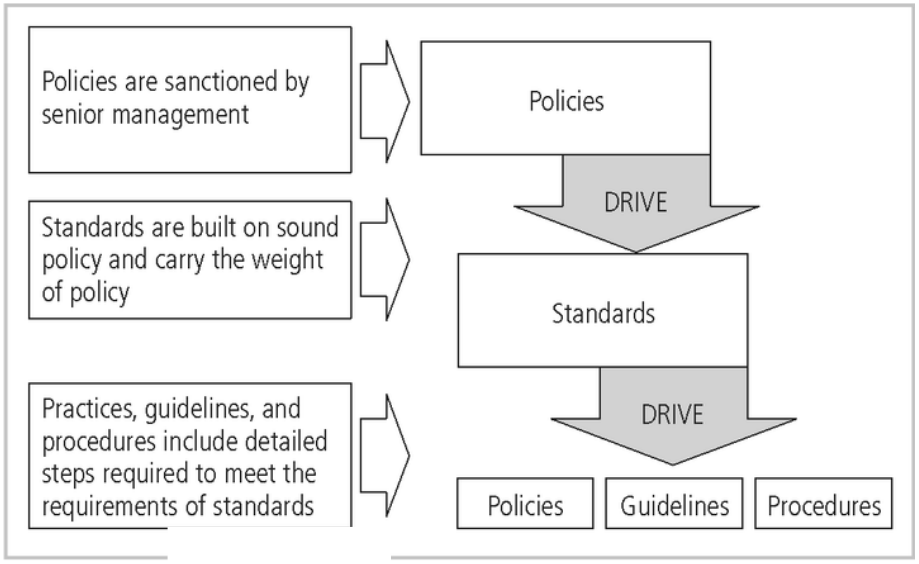
1. Threat attack identification
2. Business unit analysis
3. Attack success scenarios
4. Potential damage assessment
5. Subordinate plan classification

PART B

1) Explain how information security policy is implemented as procedure? What are the three types of security policies? Explain. (Nov /Dec 2011, May/June 2015, Nov/Dec 2014, May/June 2014)

Definitions

- **Policy**: course of action used by an organization to convey instructions from management to those who perform duties
  - Organizational rules for acceptable/unacceptable behavior
  - Penalties for violations
  - Appeals process



FIGU , Standards, and Practices

Types of Policies

1. Enterprise information Security program Policy(EISP)
2. Issue-specific information Security Policy (ISSP)
3. Systems-specific information Security Policy (SysSP)

1. Enterprise Information Security Policy (EISP)

- Also Known as a general Security policy, IT security policy, or information security policy.
- Sets strategic direction, scope, and tone for all security efforts within the organization
- Assigns responsibilities to various areas of information security
- Guides development, implementation, and management of information security program

EISP Elements

Although the specifics of EISPs vary from organization to organization, most EISP documents should include the following elements:

- An overview of the corporate philosophy on security
- Information on the structure of the information security organization and individuals who fulfill the information security role
- Fully articulated responsibilities for security that are shared by all members of the organization (employees, contractors, consultants, partners, and visitors)
- Fully articulated responsibilities for security that are unique to each role within the organization

2. Issue-Specific Security Policy (ISSP)

- The ISSP:
  - Addresses specific areas of technology
  - Requires frequent updates
  - Contains statement on position on specific issue
- Approaches to creating and managing ISSPs:
  - Create number of independent ISSP documents
  - Create a single comprehensive ISSP document
  - Create a modular ISSP document
- ISSP topics could include:
  - E-mail, use of Web, configurations of computers to defend against worms and viruses, prohibitions against hacking or testing organization security controls, home use of company-owned computer equipment, use of personal equipment on company networks, use of telecommunications technologies(FAX and phone), use of photocopiers

Components of the ISSP

- Statement of Policy
  - Scope and Applicability
  - Definition of Technology Addressed
  - Responsibilities
- Authorized Access and Usage of Equipment
  - User Access
  - Fair and Responsible Use
  - Protection of Privacy
- Prohibited Usage of Equipment
  - Disruptive Use or Misuse
  - Criminal Use
  - Offensive or Harassing Materials
  - Copyrighted, Licensed or other Intellectual Property
  - Other Restrictions
- Systems Management
  - Management of Stored Materials
  - Employer Monitoring
  - Virus Protection
  - Physical Security
  - Encryption
- Violations of Policy
  - Procedures for Reporting Violations
  - Penalties for Violations
- Policy Review and Modification
  - Scheduled Review of Policy and Procedures for Modification

- Limitations of Liability
    - Statements of Liability or Disclaimers

3. Systems-Specific Policy (SysSP)

- SysSPs are frequently codified as standards and procedures to be used when configuring or maintaining systems
- Systems-specific policies fall into two groups:
    1. **Access control lists (ACLs)**
    2. **Configuration rules**

1. Access Control Lists (ACLs):-

- **ACL** are lists, matrices, and capability tables governing the rights and privileges of a particular user to a particular system.
- An ACL is a list of access rights used by
    - File storage systems,
    - Object brokers, or
    - Other network communications devices to determine which **individuals or groups may access an object** that it controls.

Capability Table

- A similar list which is also associated with users and groups is called a **capability table**.
- This specifies which subjects and objects a user or group can access.
- Capability tables are frequently complex matrices, rather than simple lists or tables.

2. Configuration rules:-

- Comprise the specific configuration codes entered into security systems to guide the execution of the system when information is passing through it.

ACL Policies

- In general ACLs regulate the who, what, when, where, and how of access:
    - Who can use the system
    - What authorized users can access
    - When authorized users can access the system
    - Where authorized users can access the system from
    - How authorized users can access the system
- Restrictions on who can use the system require no explanation.
- Restrictions on what users can access require some detailing.
- ACLs can restrict any number of the attributes of the system resources, such as **printers, files, communications**, and **applications** by setting privileges to one of the following:
    - Read
    - Write
    - Create

- ♦ Modify
- ♦ Delete
- ♦ Compare
- ♦ Copy

Rule Policies

- Rule policies are more specific to the operation of a system than ACLs and may or may not deal with users directly.
- Many security systems require specific configuration scripts telling the systems what actions to perform on each set of information they process.
- **Examples** include
  - ➢ Firewalls,
  - ➢ Intrusion detection systems &
  - ➢ Proxy servers.

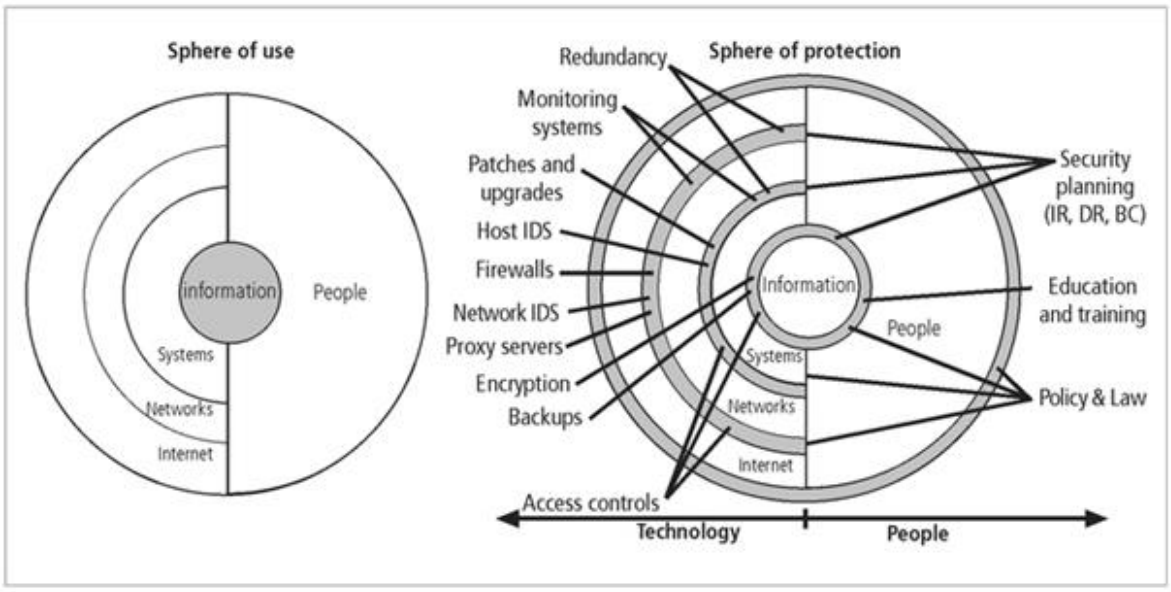
Policy Management

- Policies are living documents that must be managed and nurtured, as they constantly change and grow.
- It is unacceptable to simply create such an important set of documents and then shelve them.
- These documents must be properly
  - ➢ disseminated
  - ➢ distributed
  - ➢ read
  - ➢ understood, and
  - ➢ Agreed to and managed.
- How they are managed relates directly to the policy management section of the issue-specific policy indicated earlier.
- Good management practices for policy development and maintenance make for a more resilient organization.

2. What is Sphere of protection, Defense in Depth and Security perimeter? What are the key technological components used for security implementation? Explain in detail about design of security architecture. (Nov /Dec 2011, May/June 2015)

Sphere of Protection

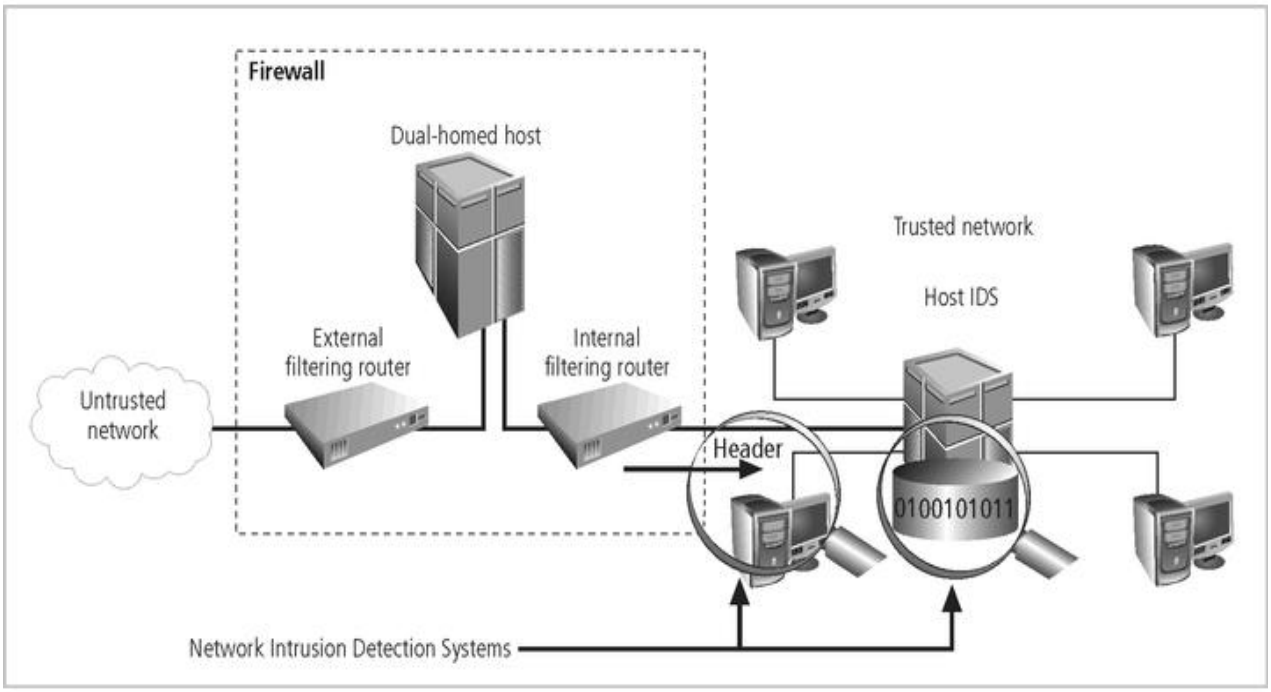
- ➢ The "sphere of protection" overlays each of the levels of the "sphere of use" with a layer of security, protecting that layer from direct or indirect use through the next layer
- ➢ The people must become a layer of security, a human firewall that protects the information from unauthorized access and use
- ➢ Information security is therefore designed and implemented in three layers
  - o policies
  - o people (education, training, and awareness programs)
  - o technology



Spheres of Security

Defense in Depth

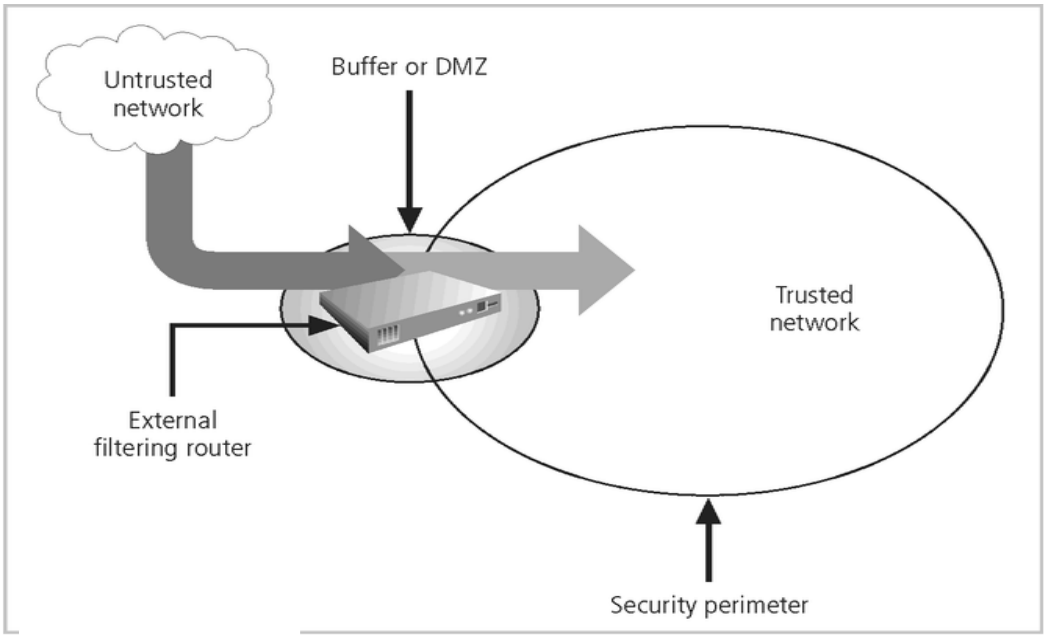
- One of the basic foundations of security architectures is the implementation of security in layers. This layered approach is called **defense in depth**.
- Defense in depth requires that the organization establish sufficient security controls and safeguards, so that an intruder faces multiple layers of controls.
- These layers of control can be organized into policy, training and education and technology as per the NSTISSC model.
- While policy itself may not prevent attacks, they coupled with other layers and deter attacks.
- Training and Education are similar.
- Technology is also implemented in layers, with detection equipment, all operating behind access control mechanisms.
- Implementing multiple types of technology and thereby preventing the failure of one system from compromising the security of the information is referred to as **redundancy**.
- Redundancy can be implemented at a number of points throughout the security architecture, such as firewalls, proxy servers, and access controls.
- The figure shows the use of firewalls and intrusion detection systems (IDS) that use both packet-level rules and data content analysis.



Defense in Depth

Security Perimeter

- The point at which an organization's security protection ends, and the outside world begins
- Referred to as the security perimeter
- Unfortunately the perimeter does not apply to internal attacks from employee threats, or on-site physical threats

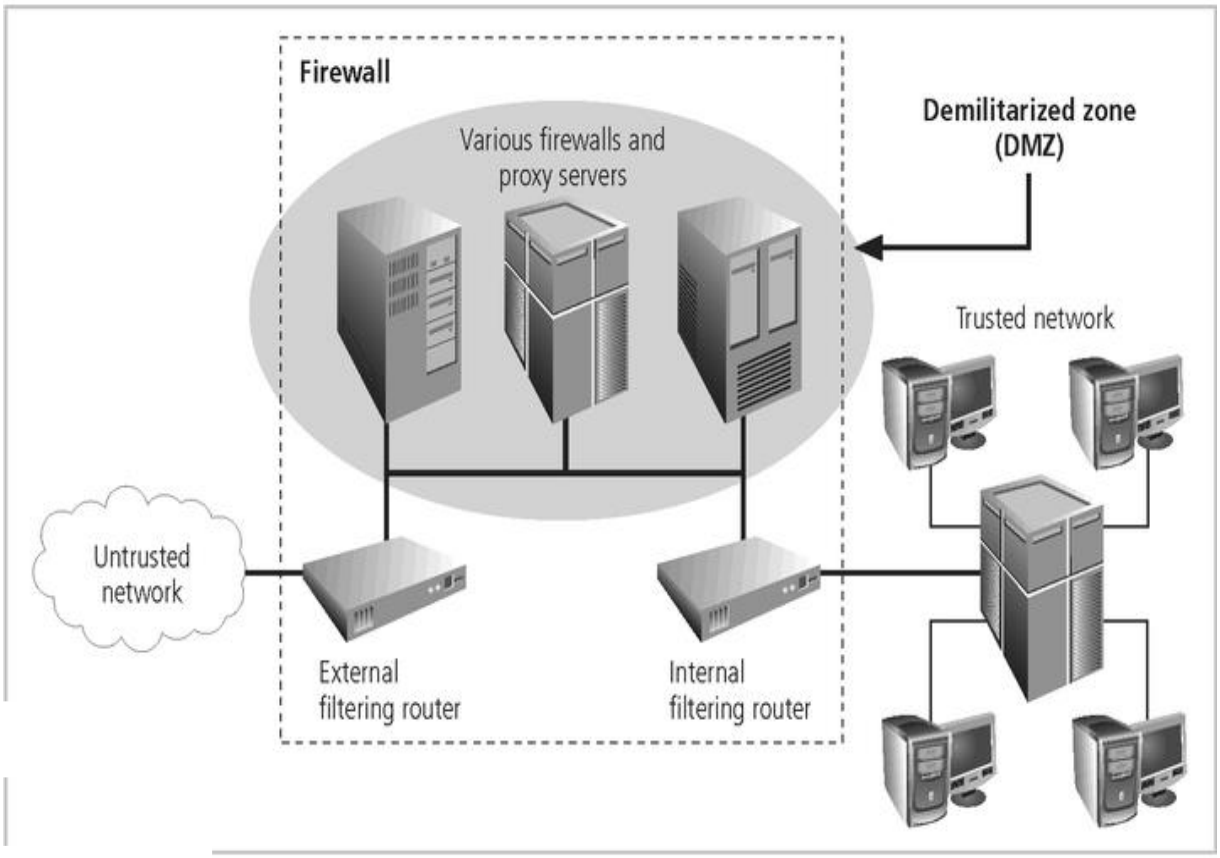


ecurity Perimeters and Domains

Key Technology Components

- Other key technology components

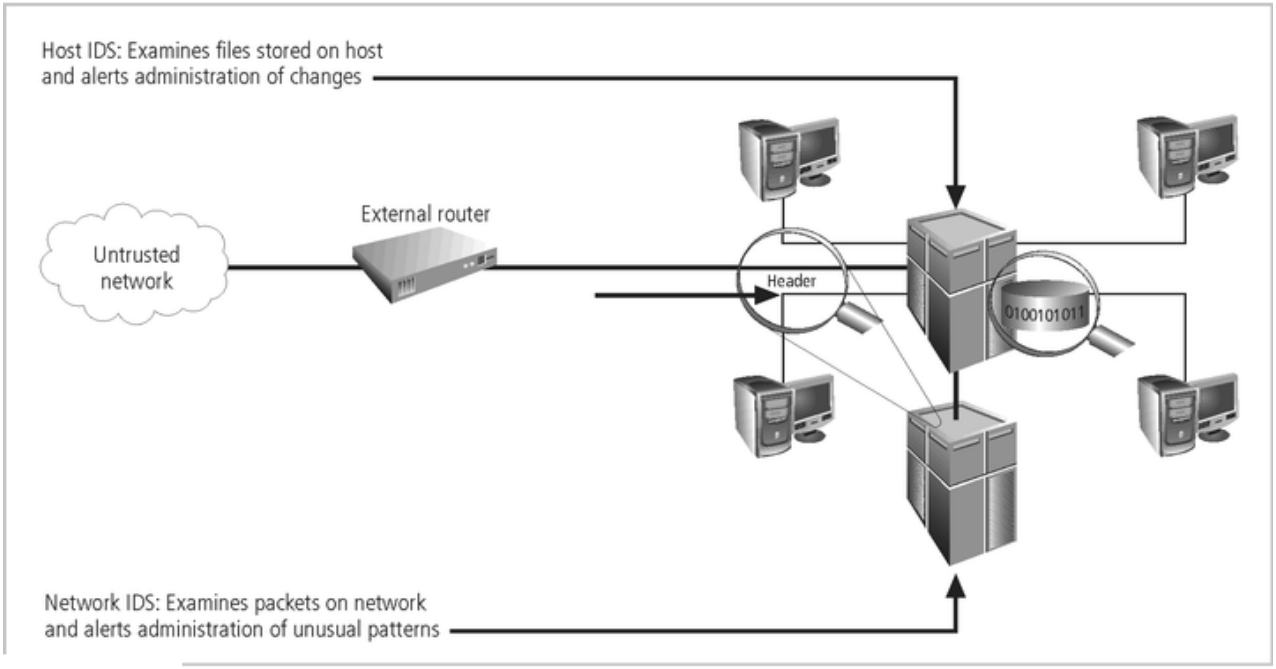
  - A **firewall** is a device that selectively discriminates against information flowing into or out of the organization.
  - Firewalls are usually placed on the security perimeter, just behind or as part of a **gateway router**.
  - Firewalls can be packet filtering, stateful packet filtering, proxy, or application level.
  - A Firewall can be a single device or a **firewall subnet**, which consists of multiple firewalls creating a buffer between the outside and inside networks.
  - The **DMZ** (demilitarized zone) is a no-man's land, between the inside and outside networks, where some organizations place Web servers
  - These servers provide access to organizational web pages, without allowing Web requests to enter the interior networks.
  - **Proxy server-** An alternative approach to the strategies of using a firewall subnet or a DMZ is to use a **proxy server**, or **proxy firewall**.
  - For more frequently accessed Web pages, proxy servers can cache or temporarily store the page, and thus are sometimes called **cache servers.**



Firewalls, Proxy Servers, and DMZs

- **Intrusion Detection Systems (IDSs).** In an effort to detect unauthorized activity within the inner network, or on individual machines, an organization may wish to implement **Intrusion Detection Systems or IDS**.
- **IDs** come in two versions. Host-based & Network-based IDSs.
  - **Host-based IDSs** are usually installed on the machines they protect to monitor the status of various files stored on those machines.
  - **Network-based IDSs** look at patterns of network traffic and attempt to detect unusual activity based on previous baselines.
- This could include packets coming into the organization's networks with addresses from machines already within the organization (IP spoofing).

- It could also include high volumes of traffic going to outside addresses (as in cases of data theft) or coming into the network (as in a denial of service attack).
- Both host-and network based IDSs require a database of previous activity.



Intrusion Detection Systems

3. Explain about VISA international security model. (NOV/DEC 2012)

VISA International Security Model

This model promotes strong security measures in its business associates and has established guidelines for the security of its information systems. It has developed two important documents

1. Security Assessment Process
2. Agreed Upon Procedures**.**

Both documents provide specific instructions on the use of the VISA Cardholder Information Security Program. The Security Assessment Process document is a series of recommendations for the detailed examination of an organization's systems with the eventual goal of integration into the VISA systems.

The Agreed upon Procedures document outlines the policies and technologies required for security systems that carry the sensitive card holder information to and

from VISA systems. Using the two documents, a security team can develop a sound strategy for the design of good security architecture. The only downside to this approach is the specific focus on systems that can or do integrate with VISA's systems with the explicit purpose of carrying the aforementioned cardholder information.

Base lining & Best Business Practices

Base lining and best practices are solid methods for collecting security practices, but provide less detail than a complete methodology. It is possible to gain information by base lining and using best practices and thus work backwards to an effective design. The Federal Agency Security Practices (FASP) site (fasp.nist.gov) designed to provide best practices for public agencies and adapted easily to private institutions. The documents found in this site include specific examples of key policies and planning documents, implementation strategies for key technologies, and position descriptions for key security personnel.

The particular value is the section on program management, which includes the following:

- A summary guide: public law, executive orders, and policy documents
- Position description for computer system security officer.
- Position description for information security officer
- Position description for computer specialist.
- Sample of an information technology(IT) security staffing plan for a large service application(LSA)
- Sample of an information technology(IT) security program policy
- Security handbook and standard operating procedures.
- Telecommuting and mobile computer security policy.

Hybrid Framework for a Blueprint of an Information Security System

The framework of security includes philosophical components of the Human Firewall Project, which maintain that people, not technology, are the primary defenders of information assets in an information security program, and are uniquely responsible for their protection. The spheres of security are the foundation of the security framework.

The sphere of use, at the left in fig, explains the ways in which people access information. For example, people read hard copies of documents and can also access information through systems. The sphere of protection at the right illustrates that between each layer of the sphere of use there must exist a layer of protection to prevent access to the inner layer from the outer layer. Each shaded band is a layer of protection and control.

4. Discuss in detail about NIST security models publications. (NOV/DEC 2014)

NIST Security Models

NIST refers to "The National Security Telecommunications and Information systems Security Committee" document. This document presents a comprehensive model for information security. Another possible approach available is described in the many documents available from the Computer Security Resource Center of the National Institute for Standards and technology. NIST documents are publicly available at no charge and have been available for some time, they have been broadly reviewed by government and industry professionals, and are among the references cited by the federal government when it decided not to select the ISO/IEC 17799 standards.

The following NIST documents can assist in the design of a security framework:

- **NIST SP 800-12 :** An Introduction to Computer Security: The NIST Handbook
- **NIST SP 800-14 :** Generally Accepted Security Principles and Practices for Securing IT Systems
- **NIST SP 800-18** : The Guide for Developing Security Plans for IT Systems
- **NIST SP 800-26**: Security Self-Assessment Guide for IT systems.
- **NIST SP 800-30**: Risk Management for IT systems.

NIST Special Publication SP 800-12

SP 800-12 is an excellent reference and guide for the security manager or administrator in the routine management of information security. It provides little guidance, however, on design and implementation of new security systems, and therefore should be used only as a valuable precursor to understanding an information security blueprint.

NIST Special Publication SP 800-14

. It provides best practices and security principles that can direct the security team in the development of **Security Blue Print**. The scope of NIST SP 800-14 is broad. It is important to consider each of the security principles it presents, and therefore the following sections examine some of the more significant points in more detail:

Security Supports the Mission of the organization

Failure to develop an information security system based on the organization's mission, vision, and culture guarantees the failure of the information security program.

Security is an integral element of Sound Management

Effective management includes planning, organizing, leading, and controlling. Security enhances management functions by providing input during the planning process for organizational initiatives. Information security controls support sound management via the enforcement of both managerial and security policies.

Security should be cost-effective

The costs of information security should be considered part of the cost of doing business, much like the cost of the computers, networks, and voice communications systems. These are not profit-generating areas of the organization and may not lead to competitive advantages. Information security should justify its own costs. The use of security measures that do not justify their cost must have a strong business justification (such as a legal requirement).

Systems Owners have security responsibilities outside their own organizations

Whenever systems store and use information from customers, patients, clients, partners, or others, the security of this information becomes the responsibility of the owner of the systems. Each system's owners are expected to diligently work with those who have systems that are interconnected with their own to assure the confidentiality, integrity, and availability of the entire value chain of interconnected systems.

Security Responsibilities and Accountability Should Be Made Explicit

Policy documents should clearly identify the security responsibilities of users, administrators, and managers. To be legally binding, the policies must be documented, disseminated, read, understood,
and agreed to by all involved members of the organization.

Security Requires a Comprehensive and Integrated approach

Security personnel alone cannot effectively implement security. Security is everyone's responsibility. The three communities of interest (information technology management and professionals, information security management and professionals, and users,managers, administrators, and other stakeholders) should participate in the process of developing a comprehensive information security program.

Security Should Be Periodically Reassessed

Information security that is implemented and then ignored is considered negligent, the organization having not demonstrated due diligence. Security is an ongoing process. To be effective against a constantly shifting set of threats and a changing user base, the security process must be periodically repeated. Continuous analyses of threats, assets, and controls must be conducted and new blueprints developed. Only thorough the preparation, design, implementation, eternal vigilance, and ongoing maintenance can secure the organization's information assets.

Security is constrained by Societal Factors

There are a number of factors that influence in the implementation and maintenance of security. Legal demands, shareholder requirements, even business practices affect the implementation of security controls and safeguards. For example, security professionals generally prefer to isolate information assets from the Internet, which is the leading avenue of threats to the assets, but the business requirements of the organization may preclude this control measure.

NIST SP 800-18

The Guide for developing Security plans for Information Technology Systems can be used as the foundation for a comprehensive security blueprint and framework. It provides detailed methods for assessing, and implementing controls and plans for applications of varying size. It can serve as a useful guide to the activities and as an aid in the planning process. It also includes templates for major application security plans

System Analysis

- System Boundaries
- Multiple similar systems
- System Categories

Plan Development All Systems

- Plan control
- System identification
- System Operational status
- System Interconnection/ Information Sharing
- Sensitivity of information handled
- Laws, regulations and policies affecting the system

Management Controls

- Risk Assessment and Management
- Review of Security Controls
- Rules of behavior
- Planning for security in the life cycle
- Authorization of Processing (Certification and Accreditation)
- System Security Plan

Operational Controls

- Personnel Security
- Physical Security
- Production, Input/Output Controls
- Contingency Planning
- Hardware and Systems Software
- Data Integrity
- Documentation
- Security Awareness, Training, and Education
- Incident Response Capability

Technical Controls

- Identification and Authentication
- Logical Access Controls
- Audit Trails

Management controls

It addresses the design and implementation of the security planning process and security program management. They also address risk management and security control reviews. They further describe the necessity and scope of legal compliance and the maintenance of the entire security life cycle.

Operational controls

It deals with the operational functionality of security in the organization. They include management functions and lower level planning, such as disaster recovery and incident response planning. They also address personnel security, physical security, and the protection of production inputs and outputs.

They guide the development of education, training and awareness programs for users, administrators, and management. Finally, they address hardware and software systems maintenance and the integrity of data.

Technical controls

It address the tactical and technical issues related to designing and implementing security in the organization, as well as issues related to examining and selecting the technologies appropriate to protecting information. They address the specifics of technology selection and the acquisition of certain technical components.

They also include logical access controls, such as identification, authentication, authorization, and accountability. They cover cryptography to protect information in storage and transit. Finally, they include the classification of assets and users, to facilitate the authorization levels needed. Using the three sets of controls, the organization should be able to specify controls to cover the entire spectrum of safeguards, from strategic to tactical, and from managerial to technical.

5. Explain in detail about contingency planning.(May/June 2014, Nov/Dec 2012)

Contingency Planning

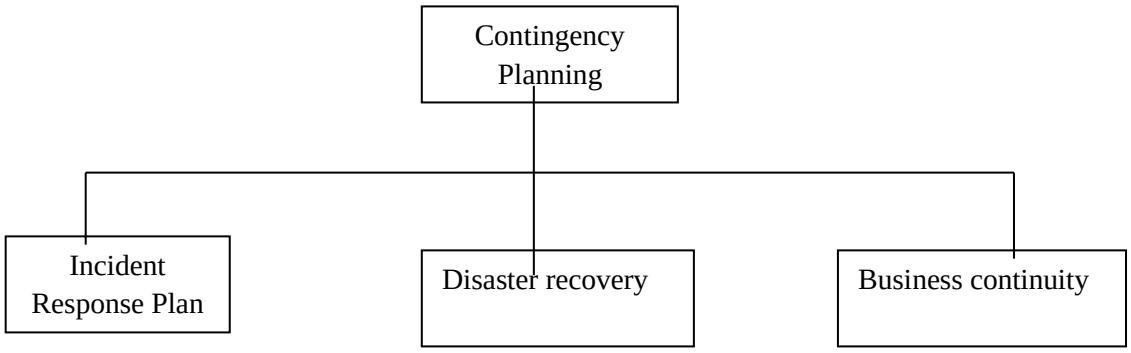
Contingency Planning (CP) comprises a set of plans designed to ensure the effective reaction and recovery from an attack and the subsequent restoration to normal modes of business operations. The organizations need to develop disaster recovery plans, incident response plans, and business continuity plans as subsets of an overall CP.

An **incident response plan (IRP)** deals with the identification, classification, response, and recovery from an incident, but if the attack is disastrous(e.g., fire, flood, earthquake) the process moves on to disaster recovery and BCP.A **disaster recovery plan (DRP)** deals with the preparation for and recovery from a disaster, whether natural or man-made and it is closely associated with BCP.

A **Business continuity plan (BCP)** ensures that critical business functions continue, if a catastrophic incident or disaster occurs. BCP occurs

concurrently with DRP when the damage is major or long term, requiring more than simple restoration of information and information resources.

Components of Contingency Planning



There are six steps to contingency planning. They are

1. Identifying the mission-or business-critical functions,
2. Identifying the resources that support the critical functions,
3. Anticipating potential contingencies or disasters,
4. Selecting contingency planning strategies,
5. Implementing the contingencies strategies,
6. Testing and revising the strategy.

1. Incident response plan (IRP)

- It is the set of activities taken to plan for, detect, and correct the impact of an incident on information assets.
- IRP consists of the following 4 phases:
    1. Incident Planning
    2. Incident Detection
    3. Incident Reaction
    4. Incident Recovery

1.1. Incident Planning

- Planning for an incident is the first step in the overall process of incident response planning.
- The planners should develop a set of documents that guide the actions of each involved individual who reacts to and recovers from the incident.
- These plans must be properly organized and stored to be available when and where needed, and in a useful format.

1.2. Incident Detection

- Incident Detection relies on either a human or automated system, which is often the help desk staff, to identify an unusual occurrence and to classify it properly as an incident.
- The mechanisms that could potentially detect an incident include intrusion detection systems (both host-based and network based), virus detection software, systems administrators, and even end users.

- Once an attack is properly identified, the organization can effectively execute the corresponding procedures from the IR plan. Thus, **incident classification** is the process of examining a potential incident, or **incident candidate**, and determining whether or not the candidate constitutes an actual incident.
- **Incident Indicators**- There is a number of occurrences that could signal the presence of an incident candidate.
- **Donald Pipkin**, an IT security expert, identifies three categories of incident indicators:
    - **Possible Indicators**
    - **Probable Indicators**
    - **Definite Indicators**

Possible Indicators- There are 4 types of possible indicators of events ,they are,

1. Presence of unfamiliar files.
2. Presence or execution of unknown programs or processes.
3. Unusual consumption of computing resources
4. Unusual system crashes

Probable Indicators- The four types of probable indicators of incidents are

1. Activities at unexpected times.
2. Presence of new accounts
3. Reported attacks
4. Notification from IDS

Definite Indicators- The five types of definite indicators of incidents are

1. Use of Dormant accounts
2. Changes to logs
3. Presence of hacker tools
4. Notifications by partner or peer
5. Notification by hacker

1.3. Incident Reaction

- It consists of actions outlined in the IRP that guide the organization in attempting to stop the incident, mitigate the impact of the incident, and provide information for recovery from the incident.
- These actions take place as soon as the incident itself is over.
- In reacting to the incident there are a number of actions that must occur quickly, including notification of key personnel and documentation of the incident.
- These must have been prioritized and documented in the IRP for quick use in the heat of the moment.

1.4. Incident Recovery

- The recovery process involves much more than the simple restoration of stolen, damaged, or destroyed data files. It involves the following steps.
  1. Identify the Vulnerabilities
  2. Address the safeguards.
  3. Evaluate monitoring capabilities
  4. Restore the data from backups.
  5. Restore the services and processes in use.
  6. Continuously monitor the system
  7. Restore the confidence of the members of the organization's communities of interest.

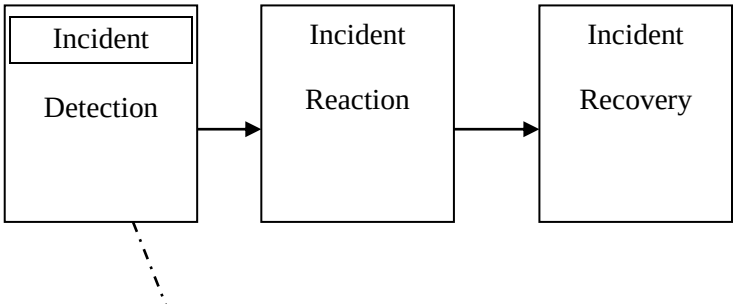
Business continuity plan

- It prepares an organization to reestablish critical business operations during a disaster that affects operations at the primary site.
- If a disaster has rendered the current location unusable for continued operations, there must be a plan to allow the business to continue to function.

Developing Continuity Programs

- Once the incident response plans and disaster recovery plans are in place, the organization needs to consider finding temporary facilities to support the continued viability of the business in the event of a disaster.
- The development of the BCP is simpler than that of the IRP and DRP ,in that it consists of selecting a continuity strategy and integrating the off-site data storage and recovery functions into this strategy.

Contingency Planning Time line



IRP

(If incident classified as Disaster)

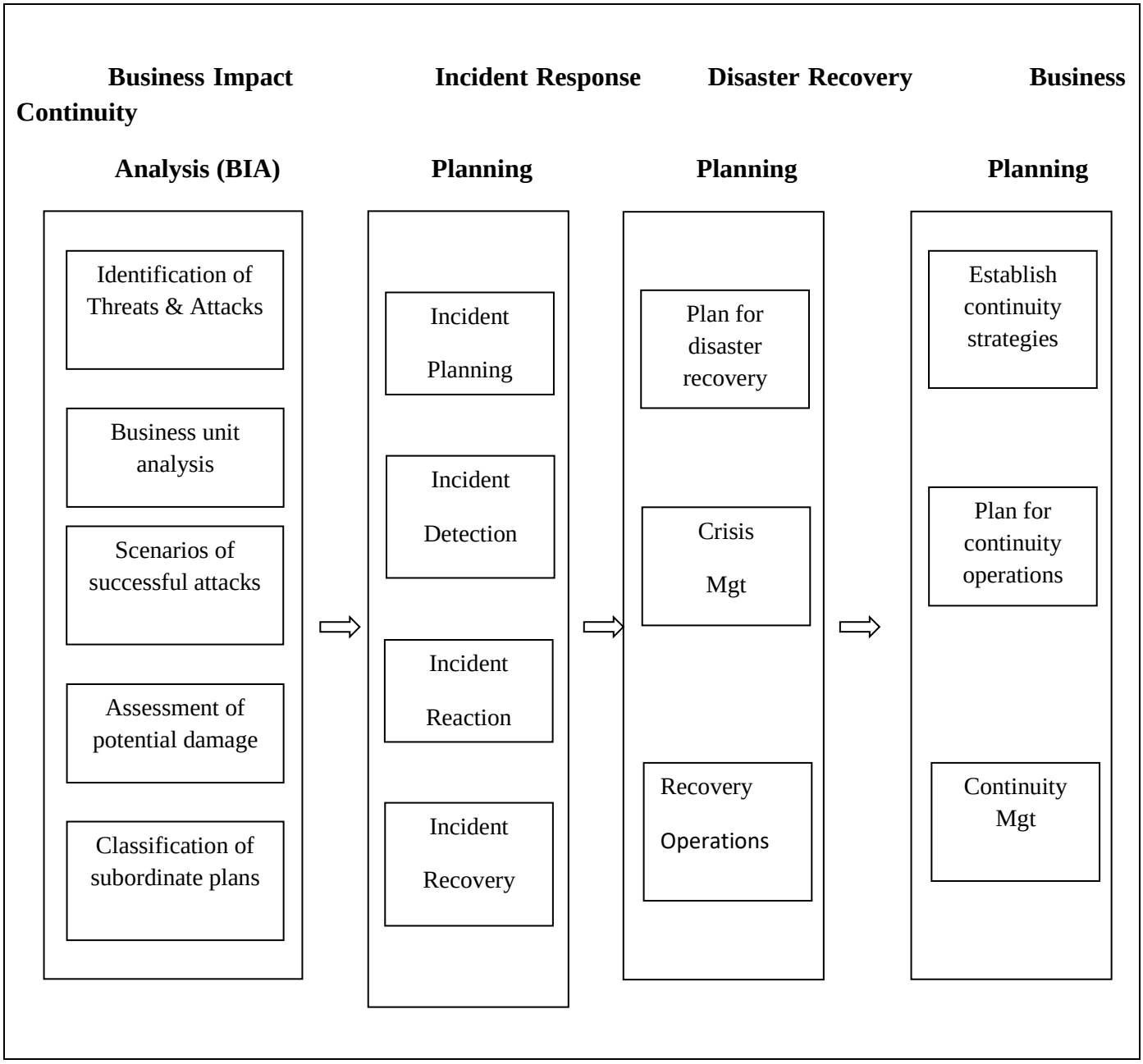
DRP

(If Disaster requires off-site operations)

BCP

Attack Occurs **Post – Attack (Hours)** **Post – attack (days)**

Major Steps in Contingency Planning



Continuity Strategies

- There are a number of strategies from which an organization can choose when planning for business continuity.
- The determining factor in selection between these options is usually cost.
- In general there are three exclusive options: Hot sites, Warm Sites, and Cold sites; and three shared functions: Time-share, Service bureaus, and Mutual Agreements.
  - **Hot sites**:

A hot site is a fully configured facility, with all services, communications links, and physical plant operations including heating and air conditioning.

- **Warm sites**:

A warm site includes computing equipment and peripherals with servers but not client work stations. It has many of the advantages of a hot site, but at a lower cost.

- **Cold Sites**:

A cold site provides only rudimentary services and facilities, No computer hardware or peripherals are provided. Basically a cold site is an empty room with heating, air conditioning, and electricity. The main advantage of cold site is in the area of cost.

- **Time-shares**:

It allows the organization to maintain a disaster recovery and business continuity option, but at a reduced overall cost. The advantages are identical to the type of site selected(hot, warm, or cold). The disadvantages are the possibility that more than one organization involved in the time share may need the facility simultaneously and the need to stock the facility with the equipment and data from all organizations involved

- **Service bureaus:**

A service bureau is an agency that provides a service for a fee. In the case of disaster recovery and continuity planning, the service is the agreement to provide physical facilities in the event of a disaster. These types of agencies also provide off-site data storage for a fee. The disadvantage is that it is a service, and must be renegotiated periodically. Also, using a service bureau can be quite expensive.

- **Mutual Agreements:**

A mutual agreement is a contract between two or more organizations that specifies how each will assist the other in the event of a disaster.

Disaster Recovery Plan (DRP)

DRP provides detailed guidance in the event of a disaster and also provides details on the roles and responsibilities of the various individuals involved in the disaster recovery effort, and identifies the personnel and agencies that must be notified. At a minimum, the DRP must be reviewed during a walk-through or talk-through on a periodic basis.

Many of the same precepts of incident response apply to disaster recovery:

1. There must be a clear establishment of priorities
2. There must be a clear delegation of roles and responsibilities
3. Someone must initiate the alert roster and notify key personnel.
4. Someone must be tasked with the documentation of the disaster.

5. If and only if it is possible, attempts must be made to mitigate the impact of the disaster on the operations of the organization.

UNIT V

PART A

1.What are firewalls?(Nov/Dec 2014)

A firewall is any device that prevents a specific type of information from moving between the un-trusted network outside and the trusted network inside the firewall may be:

- a separate computer system
- a service running on an existing router or server
- a separate network containing a number of supporting devices

2. List all physical security controls. (May/June 2013)

- guards
- dogs
- lock and keys
- electronic monitoring
- ID cards and badges
- man traps
- alarms and alarm systems

3.What is content filter? (May/June 2013)

A content filter is software filter-technically not a firewall-that allows administrators to restrict access to content from within a network. Content filtering (also known as information filtering) is the use of a program to screen and exclude from access or availability Web pages or e-mail that is deemed objectionable.

Content filtering is used by corporations as part of Internet firewall computers and also by home computer owners,

4.Distinguish between symmetric and asymmetric encryption.(Nov/Dec 2011)

Symmetric	Asymmetric
Uses the same secret (private) key to encrypt and decrypt its data	Uses both a public and private key.
Requires that the secret key be known by the party encrypting the data and the party decrypting the data.	Asymmetric allows for distribution of your public key to anyone with which they can encrypt the data they want to send securely and then it can only be Decoded by the

	person having the private key.
Fast	1000 times slower than symmetric

5. What are the seven major sources of physical loss?(Nov/Dec 2012)

- ♦ Temperature extremes
- ♦ Gases
- ♦ Liquids
- ♦ Living organisms
- ♦ Projectiles
- ♦ Movement
- ♦ Energy anomalies

6. What are Criteria for selecting information security personnel? (May/June 2012)

- General requirements
- Criminal History
- Education
- Citizenship
- Fingerprints
- Photographs
- Personal Information
- Drug Screening
- Social Security Number

7. What are the advantages and disadvantages of using honey pot or padded cell approach?(Nov/Dec 2012)

Advantages:

- ♦ Attackers can be diverted to targets that they cannot damage
- ♦ Administrators have time to decide how to respond to an attacker
- ♦ Attacker's action can be easily and extensively monitored
- ♦ Honey pots may be effective at catching insiders who are snooping around a network

Disadvantages:

- ♦ The legal implications of using such devices are not well defined
- ♦ Honey pots and Padded cells have not yet been shown to be generally useful security technologies
- ♦ An expert attacker, once diverted into a decoy system, may become angry and launch a hostile attack against an organization's systems
- ♦ Security managers will need a high level of expertise to use these systems

8. List the credentials of information security professionals. (Nov/Dec 2011)

- ISSAP – Information System Security Architecture Professional

- ISSMP - Information System Security Management Professional
- SSCP - System Security Certified Practitioner
- Security Administration
- Certified information systems security professionals (CISSP)
- Certified information systems auditor (CISA)
- Certified information security manager (CISM)
- Global information assurance certification (GIAC)

9. What is Public Key Infrastructure (PKI)?

PKI or Public Key Infrastructure

- Public Key Infrastructure is the entire set of hardware, software,
- Cryptosystems necessary to implement public key encryption
- PKI systems are based on public-key cryptosystems and include digital certificates and certificate authorities (CAs) and can:

  Issue digital certificates

  Issue crypto keys

10. What are Digital signatures? (May/June 2015)

- An interesting thing happens when the asymmetric process is reversed, that is the private key is used to encrypt a short message
- The public key can be used to decrypt it, and the fact that the message was sent by the organization that owns the private key cannot be reputed
- This is known as non-repudiation, which is the foundation of digital signatures
- Digital Signatures are encrypted messages that are independently verified by a central facility (registry) as authentic

11. What is a honey pot? (APRIL/MAY 2008)

Honey pot is a system designed to learn how "black hats" probe for and exploit weaknesses in an IT system It can also be defined as an information system resource whose value lies in unauthorized or illicit use of that resource. A honey pot is a decoy, put out on a network as bait to lure attackers.

12. Mention the categories of IDS. (NOV/DEC 2007)

a) Network-based IDS
b) Host-based IDS
c) Application-based IDS
d) Signature-based IDS
e) Statistical Anomaly-Based IDS(Also called Behavior-based IDS)
f) Log File Monitors(LFM)

13. What are the basic functions of access control devices? (NOV/DEC 2007)

Access control devices can be used to regulate who or what can view or use resources in a computing environment. Access control is the collection of mechanisms that permits managers of a system to exercise a directing or restraining influence over the behavior, use, and content of a system.

- Authentication
- Authorization
- Permit.
- Restrict

PART B

1.Explain the generations and different types of firewalls. (May/June 2015, May/June 2014)

Firewalls

A firewall is any device that prevents a specific type of information from moving between the untrusted network outside and the trusted network inside. There are five recognized generations of firewalls. The firewall may be a separate computer system, service running on an existing router or server, separate network containing a number of supporting devices.

First Generation

It is called as packet filtering firewalls and it also examines every incoming packet header and selectively filters packets based on the address, packet type, port request, and other factors. The restrictions most commonly implemented are based on:

- IP source and destination address
- Direction (inbound or outbound)
- TCP or UDP source and destination port-requests

Second Generation

It is also called as application-level firewall or proxy server. Often a dedicated computer separate from the filtering router. With this configuration the proxy server, rather than the Web server, is exposed to the outside world. Additional filtering routers can be implemented behind the proxy server. The primary disadvantage of application-level firewalls is that they are designed

for a specific protocol and cannot easily be reconfigured to protect against attacks on protocols for which they are not designed

Third Generation

It is called stateful inspection firewalls. It keeps track of each network connection established between internal and external systems using a state table which tracks the state and context of each packet. If the stateful firewall receives an incoming packet that it cannot match in its state table, then it defaults to its ACL to determine whether to allow the packet to be passed. The primary disadvantage is the additional processing requirements of managing and verifying packets against the state table which can possibly expose the system to a DOS attack. These firewalls can track connectionless packet traffic such as UDP and remote procedure calls (RPC) traffic

Fourth Generation

While static filtering firewalls, such as first and third generation, allow entire sets of one type of packet to enter in response to authorized requests, a dynamic packet filtering firewall allows only a particular packet with a particular source, destination, and port address to enter through the firewall .It is done by understanding how the protocol functions, and opening and closing "doors" in the firewall, based on the information contained in the packet header. In this manner, dynamic packet filters are an intermediate form, between traditional static packet filters and application proxies.

Fifth Generation

The final form of firewall is the kernel proxy, a specialized form that works under the Windows NT Executive, which is the kernel of Windows NT evaluates packets at multiple layers of the protocol stack, by checking security in the kernel as data is passed up and down the stack.

The five processing modes are:

1) Packet filtering
2) Application gateways
3) Circuit gateways
4) MAC layer firewalls
5) Hybrids

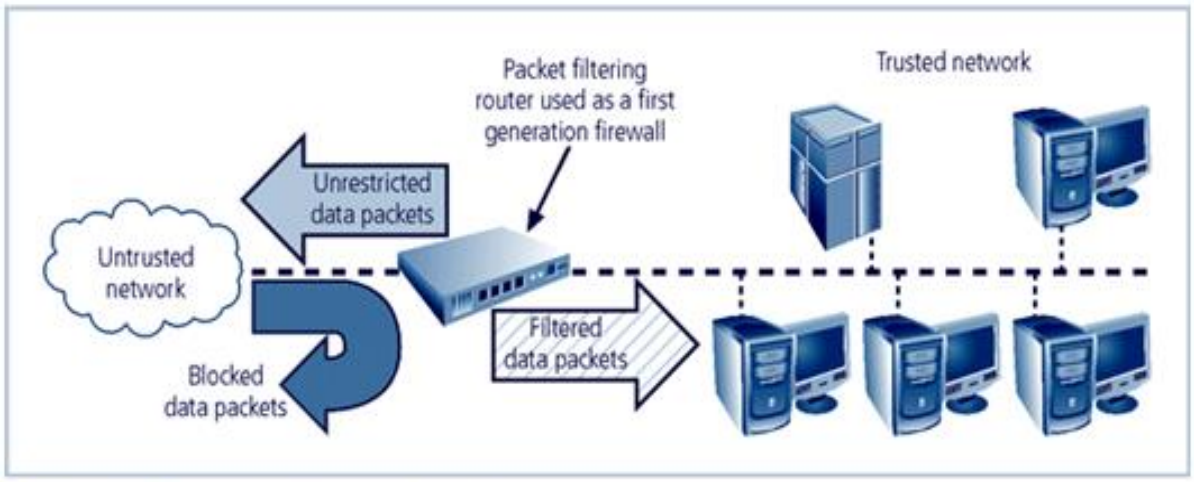
Packet-filtering Routers

Most organizations with an Internet connection have some form of a router as the interface at the perimeter between the organization's internal networks and the external service provider. Many of these routers can be configured to filter packets that the organization does not allow into the network

.This is a simple but effective means to lower the organization's risk to external attack.
The drawback to this type of system includes a lack of auditing and strong authentication. The complexity of the access control lists used to filter the packets can grow and degrade network performance

Packet-filtering Routers

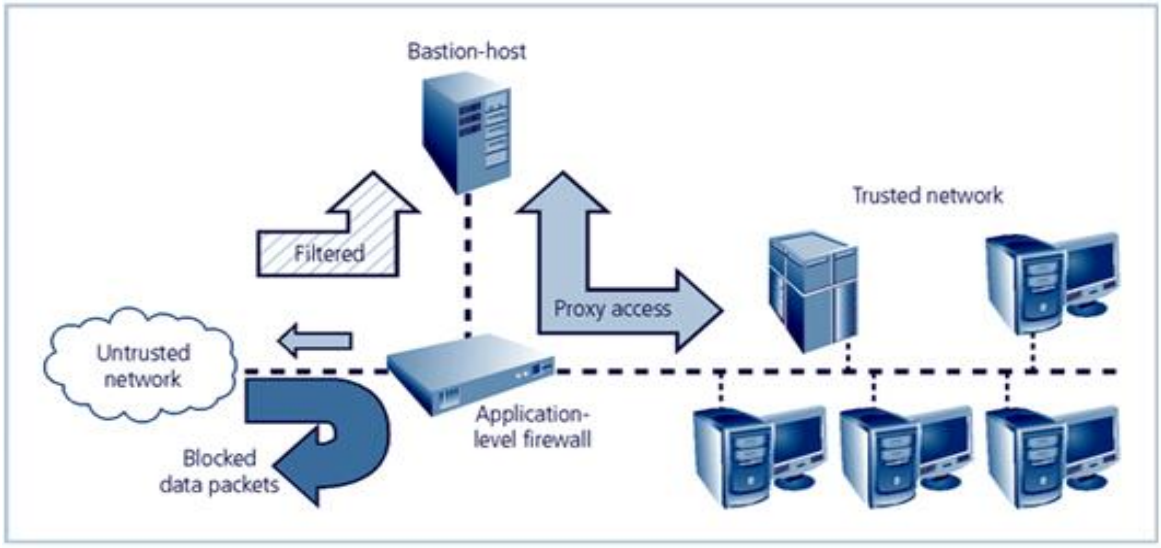
- Most organizations with an Internet connection have some form of a router as the interface at the perimeter between the organization's internal networks and the external service provider
- Many of these routers can be configured to filter packets that the organization does not allow into the network
- This is a simple but effective means to lower the organization's risk to external attack
- The drawback to this type of system includes a lack of auditing and strong authentication
- The complexity of the access control lists used to filter the packets can grow and degrade network performance



Packet Filtering Firewall

Screened-Host Firewall Systems

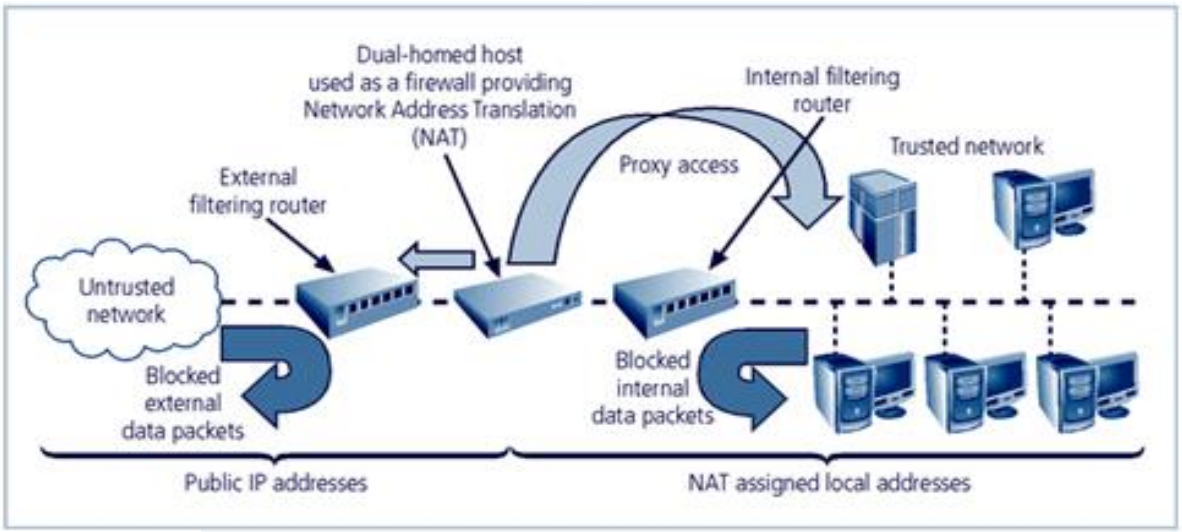
- Combine the packet-filtering router with a separate, dedicated firewall such as an application proxy server
- Allows the router to pre-screen packets to minimize the network traffic and load on the internal proxy
- Application proxy examines an application layer protocol, such as HTTP, and performs the proxy services
- This separate host is often referred to as a bastion-host, as it represents a single, rich target for external attacks, and should be very thoroughly secured



Screened Host Firewall

Dual-homed Host Firewalls

- The bastion-host contains two NICs (network interface cards)
- One NIC is connected to the external network, and one is connected to the internal network
- With two NICs all traffic must physically go through the firewall to move between the internal and external networks
- A technology known as network-address translation (NAT) is commonly implemented with this architecture to map from real, valid, external IP addresses to ranges of internal IP addresses that are non-routable

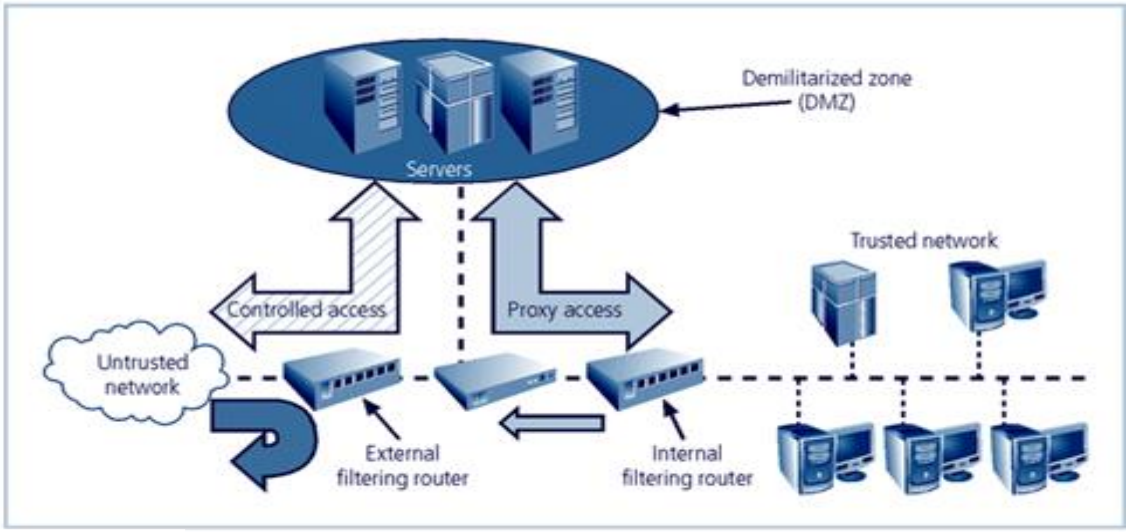


Dual-homed Host Firewall

ıbnet Firewalls (with DMZ)

- Consists of two or more internal bastion-hosts, behind a packet-filtering router, with each host protecting the trusted network
- The first general model consists of two filtering routers, with one or more dual-homed bastion-host between them

- The second general model involves the connection from the outside or untrusted network going through this path:
  - Through an external filtering router
  - Into and then out of a routing firewall to the separate network segment known as the DMZ
- Connections into the trusted internal network are allowed only from the DMZ bastion-host servers



Screened Subnet (DMZ)

Selecting the Right Firewall

- What type of firewall technology offers the right balance of protection features and cost for the needs of the organization?
- What features are included in the base price? What features are available at extra cost? Are all cost factors known?
- How easy is it to set up and configure the firewall? How accessible are staff technicians with the mastery to do it well?
- Can the candidate firewall adapt to the growing network in the target organization?

SOCKS Servers

- The SOCKS system is a proprietary circuit-level proxy server that places special SOCKS client-side agents on each workstation
- Places the filtering requirements on the individual workstation, rather than on a single point of defense (and thus point of failure)
- This frees the entry router of filtering responsibilities, but then requires each workstation to be managed as a firewall detection and protection device
- A SOCKS system can require additional support and management resources to configure and manage possibly hundreds of individual clients, versus a single device or set of devices

Firewall Recommended Practices

- All traffic from the trusted network is allowed out

- The firewall device is always inaccessible directly from the public network
- Allow Simple Mail Transport Protocol (SMTP) data to pass through your firewall, but insure it is all routed to a well-configured SMTP gateway to filter and route messaging traffic securely
- All Internet Control Message Protocol (ICMP) data should be denied
- Block telnet (terminal emulation) access to all internal servers from the public networks
- When Web services are offered outside the firewall, deny HTTP traffic from reaching your internal networks by using some form of proxy access or DMZ architecture

2. What are intrusion detection systems (IDS)? (Nov /Dec 2011, May/June 2015, Nov/Dec 2014, Nov/Dec 2012, May/June 2013)

Intrusion Detection Systems (IDSs)

IDSs work like burglar alarms. IDSs require complex configurations to provide the level of detection and response desired. An IDS operates as either network-based, when the technology is focused on protecting network information assets, or host-based, when the technology is focused on protecting server or host information assets. IDSs use one of two detection methods, signature-based or statistical anomaly-based.

IDS terminology

- Alert or alarm
- False negative - The failure of an IDS system to react to an actual attack event.
- False positive - An alarm or alert that indicates that an attack is in progress or that an attack has successfully occurred when in fact there was no such attack.
- Confidence value
- Alarm filtering

IDSs Classification

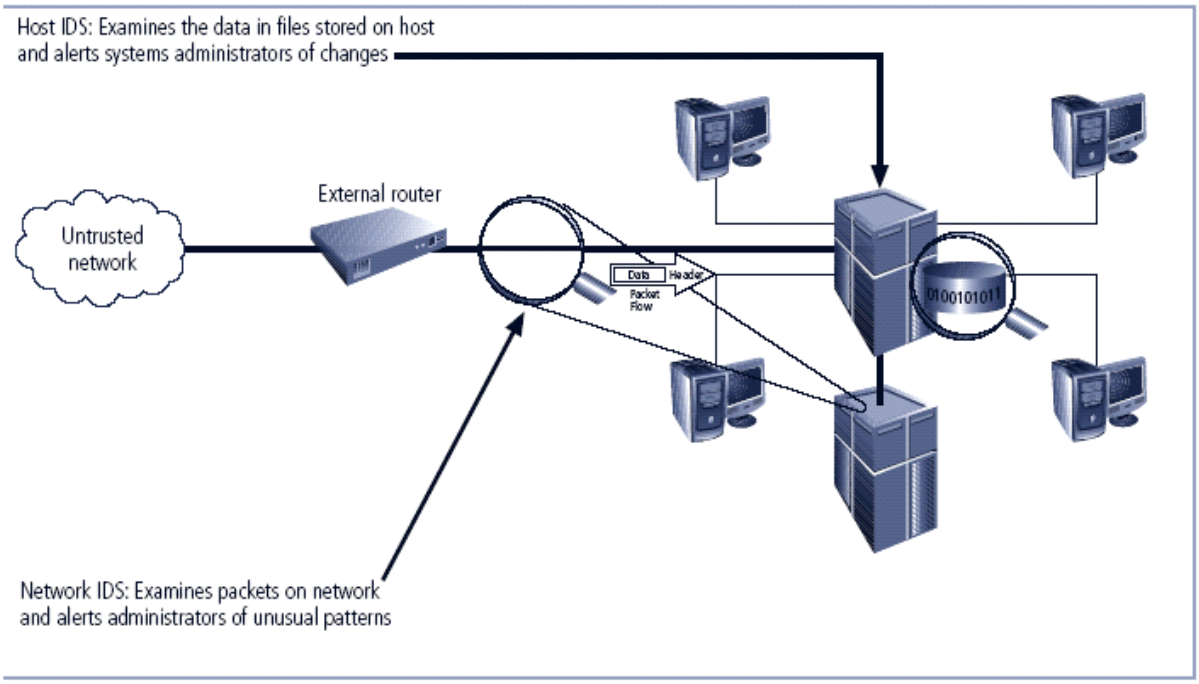
- All IDSs use one of two detection methods:
  - Signature-based
  - Statistical anomaly-based
- IDSs operate as:
  - Network-based
  - Host-based
  - Application-based systems

1. Signature-Based IDS

- Examine data traffic in search of patterns that match known signatures
- Widely used because many attacks have clear and distinct signatures
- Problem with this approach is that as new attack strategies are identified, the IDS's
  Database of signatures must be continually updated

2. Statistical Anomaly-Based IDS

- The statistical anomaly-based IDS (stat IDS) or behavior-based IDS sample network activity to compare to traffic that is known to be normal
- When measured activity is outside baseline parameters or clipping level, IDS will trigger an alert
- IDS can detect new types of attacks
- Requires much more overhead and processing capacity than signature-based
- May generate many false positives



Intrusion Detection Systems

3. Network-Based IDS (NIDS)

- Resides on computer or appliance connected to segment of an organization's network;
- When examining packets, a NIDS looks for attack patterns
- Installed at specific place in the network where it can watch traffic going into and out of particular network segment

NIDS Signature Matching

- To detect an attack, NIDSs look for attack patterns
- Done by using special implementation of TCP/IP stack:
  - In process of protocol stack verification, NIDSs look for invalid data packets
  - In application protocol verification, higher-order protocols are examined for unexpected packet behavior or improper use

4. Host-Based IDS

- Host-based IDS (HIDS) resides on a particular computer or server and monitors activity only on that system
- Benchmark and monitor the status of key system files and detect when intruder creates, modifies, or deletes files
- Most HIDSs work on the principle of configuration or change management
- Advantage over NIDS: can usually be installed so that it can access information encrypted when traveling over network

5. Application-Based IDS

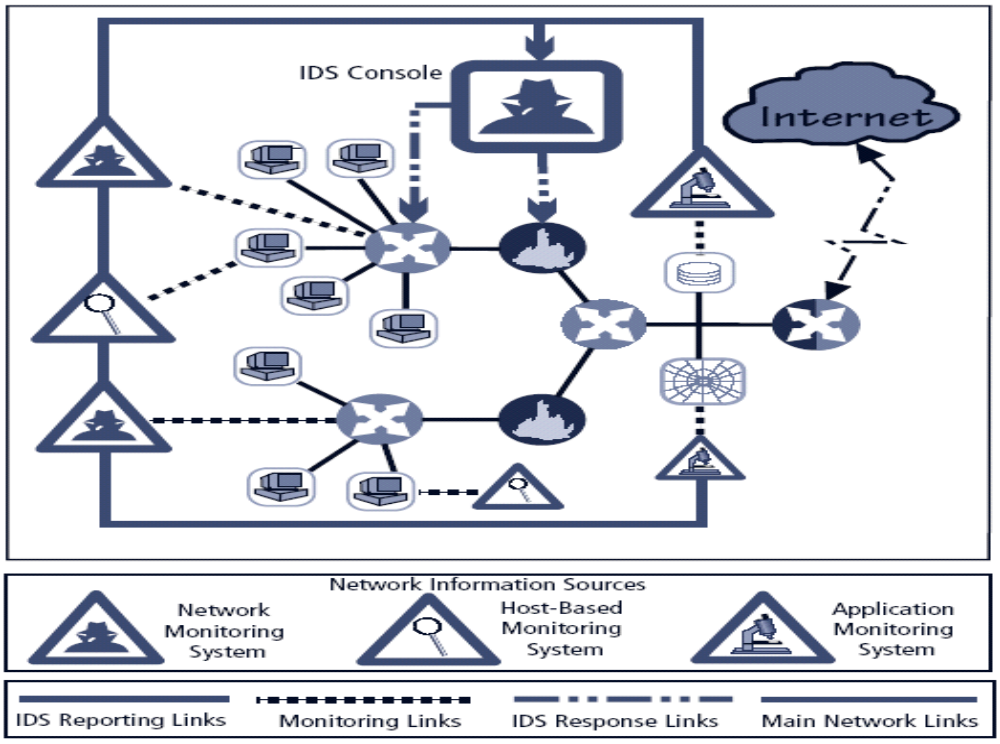
- Application-based IDS (AppIDS) examines application for abnormal events
- AppIDS may be configured to intercept requests:
  - File System
  - Network
  - Configuration
  - Execution Space

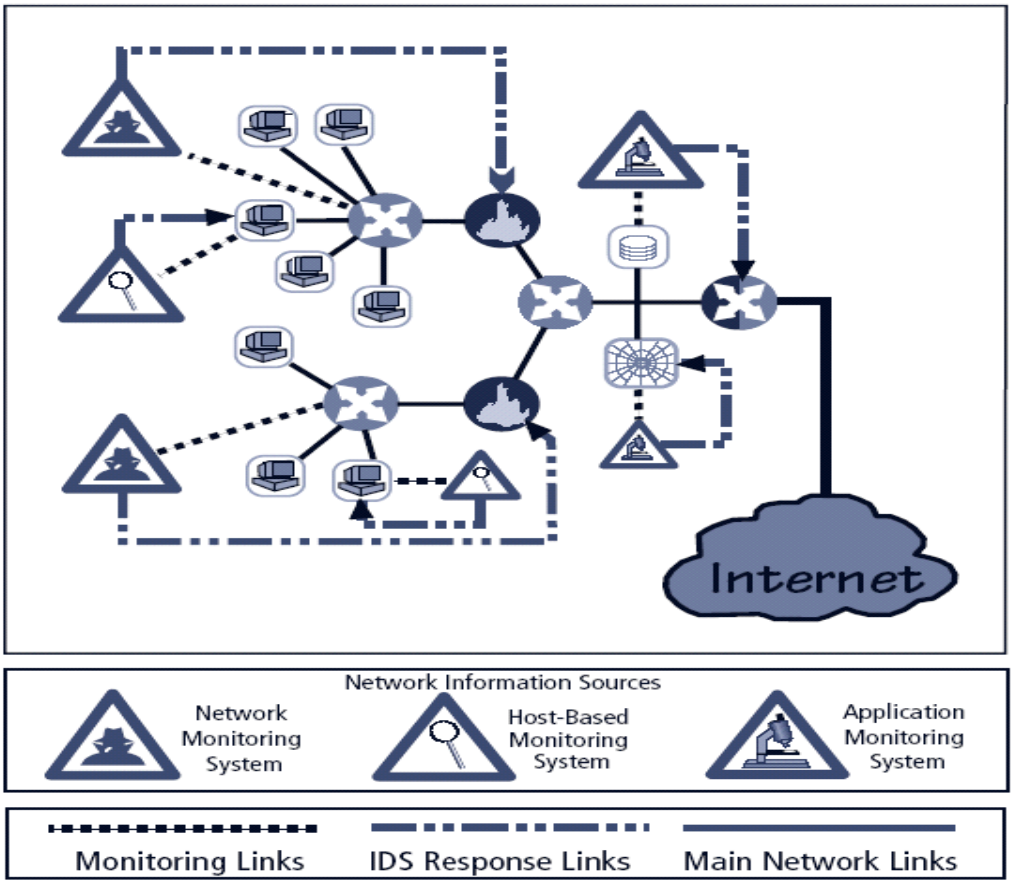
6. Log File Monitors (LFM)

Log File Monitor (LFM) is an approach to IDS that is similar to NIDS. The system reviews the log files generated by servers, network devices These systems look for patterns and signatures in the log files that may indicate an attack or intrusion is in process or has already succeeded.

IDS Control Strategies

- An IDS can be implemented via one of three basic control strategies
  - Centralized: all IDS control functions are implemented and managed in a central location
  - Fully distributed: all control functions are applied at the physical location of each
    IDS component
  - Partially distributed: combines the two; while individual agents can still analyze and respond to local threats, they report to a hierarchical central facility to enable organization to detect widespread attacks



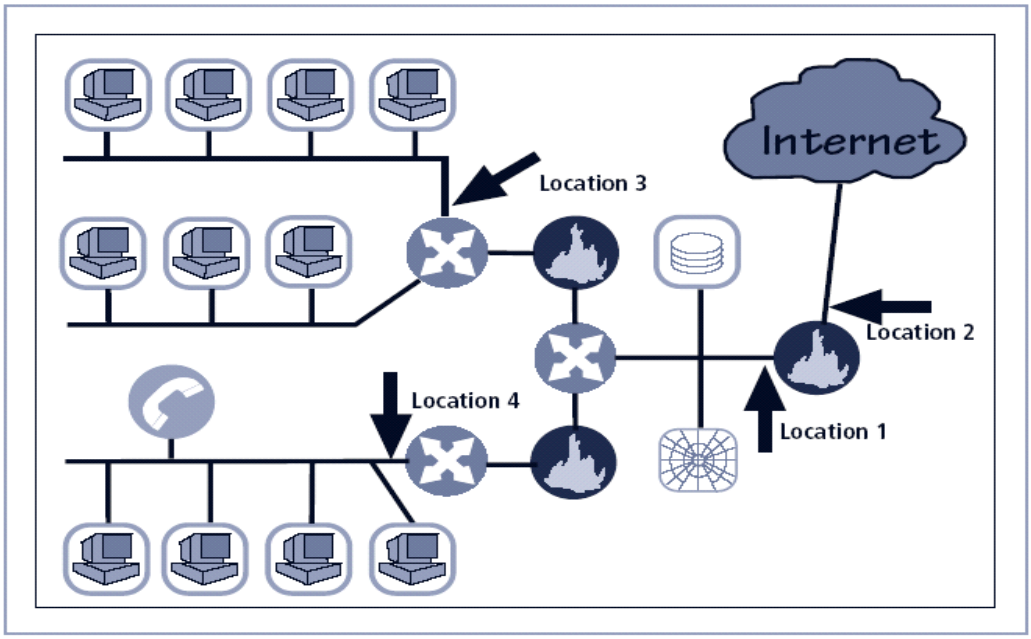


Deploying Network-Based IDSs

NIST recommends four locations for NIDS sensors

- Location 1: behind each external firewall, in the network DMZ

- Location 2: outside an external firewall
- Location 3: On major network backbones
- Location 4: On critical subnets



FIGU rk IDS Sensor Locations[17]

Honey Pots, Honey Nets, and Padded Cell Systems

- Honey pots: decoy systems designed to lure potential attackers away from critical systems and encourage attacks against the themselves
- Honey nets: collection of honey pots connecting several honey pot systems on a subnet
- Honey pots designed to:
  - Divert attacker from accessing critical systems
  - Collect information about attacker's activity
  - Encourage attacker to stay on system long enough for administrators to document event and, perhaps, respond

Trap and Trace Systems

- Use combination of techniques to detect an intrusion and trace it back to its source
- Trap usually consists of honey pot or padded cell and alarm
- Legal drawbacks to trap and trace
  - Enticement: process of attracting attention to system by placing tantalizing bits of information in key locations
  - Entrapment: action of luring an individual into committing a crime to get a conviction.

3. How Scanning and Analysis tools are useful in enforcing Information Security?

Explain different types of the Scanning and Analysis tools available. (Nov /Dec 2011)

- Scanners, sniffers, and other analysis tools are useful to security administrators in enabling them to see what the attacker sees
- Scanner and analysis tools can find vulnerabilities in systems
- One of the preparatory parts of an attack is known as foot printing – collecting IP addresses and other useful data
- The next phase of pre-attack data gathering process is called fingerprinting – scanning all known addresses to make a network map of the target

The attack protocol is a series of steps or processes used by an attacker, in a logical sequence to launch an attack against a target system or networks. One of the preparatory part of the attack protocol is the collection of publicly available information about a potential target, a process known **as** foot printing.

Foot printing

- Foot printing is the organized research of the Internet addresses owned or controlled by the target organization. The attacker uses public Internet data sources to perform keyword searches to identify the network addresses of the organization. This research is augmented by browsing the organization's web pages.
- The next phase of the attack protocol is a second intelligence or data-gathering process called **fingerprinting.** This is systematic survey of all of the target organization's **Internet addresses (**which are collected during the foot printing phase); the survey is conducted to ascertain the network services offered by the hosts in that range.
- Fingerprinting reveals useful information about the internal structure and operational nature of the target system or network for the anticipated attack.

Port Scanners

- Port scanners fingerprint networks to find ports and services and other useful information
- Why secure open ports?
    - An open port can be used to send commands to a computer, gain access to a server, and exert control over a networking device
    - The general rule of thumb is to remove from service or secure any port not absolutely necessary for the conduct of business

Vulnerability Scanners

- Vulnerability scanners are capable of scanning networks for very detailed information
- As a class, they identify exposed usernames and groups, show open network shares, expose configuration problems, and other vulnerabilities in servers

Packet Sniffers

- A network tool that collects copies of packets from the network and analyzes them
- Can be used to eavesdrop on the network traffic
- To use a packet sniffer legally, you must be:
    - on a network that the organization owns
    - under direct authorization of the owners of the network
    - have knowledge and consent of the content creators (users**)**

Content Filters

- Although technically not a firewall, a content filter is a software filter that allows administrators to restrict accessible content from within a network
- The content filtering restricts Web sites with inappropriate content

Trap and Trace

- Trace: determine the identity of someone using unauthorized access
- Better known as honey pots, they distract the attacker while notifying the administrator

Wireless Security Tools

- Organization that spends its time securing wired network and leaves wireless networks to operate in any manner is opening itself up for security breach.
- A wireless security toolkit should include the ability to sniff wireless traffic, scan wireless hosts, and assess level of privacy or confidentiality afforded on the wireless network

Firewall Analysis Tools

- Several tools automate remote discovery of firewall rules and assist the administrator in analyzing the rules
- Administrators who feel wary of using same tools that attackers use should remember:
    - It is intent of user that will dictate how information gathered will be used
- A tool that can help close up an open or poorly configured firewall will help network defender minimize risk from attack

4. What is Cryptography? Explain the key terms associated with cryptography. Explain briefly the basic Encryption Definitions. (Nov /Dec 2011)

- **Cryptography** ,which comes from the Greek work kryptos ,meaning "hidden",and graphein, meaning "to write", is process of making and using codes to secure the transmission of information.
- **Crypto-analysis** is the process of obtaining the original message (called plaintext) from an encrypted message (called the cipher text) without knowing the algorithms and keys used to perform the encryption.
- **Encryption** is the process of converting an original message into a form that is unreadable to unauthorized individuals-that is; to anyone without the tools to convert the encrypted message back to its original format.

- **Decryption** is the process of converting the cipher text into a message that conveys readily understood meaning.

Encryption Definitions

- **Algorithm:** the mathematical formula used to convert an unencrypted message into an encrypted message**.**
- **Cipher:** the transformation of the individual components (characters, bytes, or bits) of an unencrypted message into encrypted components**.**
- **Cipher-text or cryptogram:** the unintelligible encrypted or encoded message resulting from an encryption.
- **Code:** the transformation of the larger components (words or phrases) of an unencrypted message into encrypted components**.**
- **Cryptosystem:** the set of transformations necessary to convert an unencrypted message into an encrypted message**.**
- **Decipher**: to decrypt or convert cipher text to plaintext**.**
- **Encipher**: to encrypt or convert plaintext to ciph**er text.**
- **Key or crypto variable:** the information used in conjunction with the algorithm to create cipher text from plaintext.
- **Key space:** the entire range of values that can possibly be used to construct an individual key.
- **Link encryption:** a series of encryptions and decryptions between a number of systems, whereby each node decrypts the message sent to it and then re-encrypts it using different keys and sends it to the next neighbor, until it reaches the final destination.
- **Plaintext:** the original unencrypted message that is encrypted and results from successful decryption**.**
- **Steganography:** the process of hiding messages in a picture or graphic**.**
- **Work factor:** the amount of effort (usually in hours) required to perform cryptanalysis on an encoded message**.**

Data Encryption Standard (DES)

- Developed in 1977 by IBM
- Based on the Data Encryption Algorithm (DEA)
- Uses a 64-bit block size and a 56-bit key
- With a 56-bit key, the algorithm has 256 possible keys to choose from (over 72 quadrillion)
- DES is a federally approved standard for non classified data
- DES was cracked in 1997 when RSA put a bounty on the algorithm offering $10,000 to the team to crack the algorithm - fourteen thousand users collaborated over the Internet to finally break the encryption

Triple DES (3DES)

- Developed as an improvement to DES
- Uses up to three keys in succession and also performs three different encryption operations:

- 3DES encrypts the message three times with three different keys, the most secure level of encryption possible with 3DES

- In 1998, it took a dedicated computer designed by the Electronic Freedom Frontier (www.eff.org) over 56 hours to crack DES
- The successor to 3DES is Advanced Encryption Standard (AES), based on the Rijndael Block Cipher, a block cipher with a variable block length and a key length of either128, 192, or 256 bits
- It would take the same computer approximately 4,698,864 quintillion years to crack AES

Digital Signatures

- An interesting thing happens when the asymmetric process is reversed, that is the private key is used to encrypt a short message
- The public key can be used to decrypt it, and the fact that the message was sent by the organization that owns the private key cannot be refuted
- This is known as non-repudiation, which is the foundation of digital signatures
- Digital Signatures are encrypted messages that are independently verified by a central facility (registry) as authentic

PKI or Public Key Infrastructure : Public Key Infrastructure is the entire set of hardware, software, and cryptosystems necessary to implement public key encryption**.**PKI systems are based on public-key cryptosystems and include digital certificates and certificate authorities (CAs) and can:

- Issue digital certificates
- Issue crypto keys
- Provide tools to use crypto to secure information
- Provide verification and return of certificates

PKI Benefits

PKI protects information assets in several ways:

- Authentication
- Integrity
- Privacy
- Authorization
- Non repudiation

5. Discuss the cryptographic tools used for providing the security.(NOV/DEC 2011)

The ability to conceal the contents of sensitive messages and to verify the contents of messages and the identities of their senders have the potential to be useful in all areas of business. To be actually useful, these cryptographic capabilities must be

embodied in tools that allow IT and information security practitioners to apply the elements of cryptography in the everyday.

Public-key Infrastructure (PKI) is an integrated system of software, encryption methodologies, protocols, legal agreements, and third-party services that enables users to communicate securely. PKI systems are based on public-key cryptosystems and include digital certificates and certificate authorities (CAs).

Digital certificates are public-key container files that allow computer programs to validate the key and identify to whom it belongs. (More information about digital certificates appears in later sections of this chapter.) PKI and the digital certificate registries they contain enable the protection of information assets by making verifiable digital certificates readily available to business applications. This, in turn, allows the applications to implement several of the key characteristics of information security and to integrate these characteristics into business processes across an organization. These processes include the following:

Authentication: Individuals, organizations, and Web servers can validate the identity of each of the parties in an Internet transaction.

Integrity: Content signed by the certificate is known to not have been altered while in transit from host to host or server to client.

Privacy: Information is protected from being intercepted during transmission.

Authorization: The validated identity of users and programs can enable authorization rules that remain in place for the duration of a transaction; this reduces some of the overhead and allows for more control of access privileges for specific transactions.

Non repudiation: Customers or partners can be held accountable for transactions, such as online purchases, which they cannot later dispute. A typical PKI solution protects the transmission and reception of secure information by integrating the following components: A **certificate authority (CA)**, which issues, manages, authenticates, signs, and revokes users' digital certificates, which typically contain the user name, public key, and other identifying information.

A **registration authority (RA)**, which operates under the trusted collaboration of the certificate authority and can handle day-to-day certification functions, such as verifying registration information, generating end-user keys, revoking certificates, and validating user certificates. Certificate directories, which are central locations for certificate storage that provide a single access point for administration and distribution.

Management protocols, which organize and manage the communications among CAs,RAs, and end users. This includes the functions and procedures for setting up new users, issuing keys, recovering keys, updating keys, revoking keys, and enabling the transfer of certificates and status information among the parties involved in the PKI's area of authority. Policies and procedures, which assist an organization in the

application and management of certificates, in the formalization of legal liabilities and limitations, and in actual business use.

Common implementations of PKI include systems that issue digital certificates to users and servers directory enrollment key issuing systems; tools for managing the key issuance and verification and return of certificates. These systems enable organizations to apply an enterprise-wide solution that provides users within the PKI's area of authority the means to engage in authenticated and secure communications and transactions.

Digital signatures

Digital Signatures were created in response to the rising need to verify information transferred via electronic systems. Asymmetric encryption processes are used to create digital signatures. When an asymmetric cryptographic process uses the sender's private key to encrypt a message, the sender's public key must be used to decrypt the message. When the decryption is successful, the process verifies that the message was sent by the sender and thus cannot be refuted. This process is known as **non repudiation** and is the principle of cryptography that underpins the authentication mechanism collectively known as a digital signature. Digital signatures are, therefore, encrypted messages that can be mathematically proven authentic.

These algorithms can be used in conjunction with the sender's public and private keys, the receiver's public key, and the Secure Hash Standard (described earlier in this chapter) to quickly create messages that are both encrypted and non repudiable. This process first creates a message digest using the hash algorithm, which is then input into the digital signature algorithm along with a random number to generate the digital signature. The digital signature function also depends upon the sender's private key and other information provided by the CA. The resulting encrypted message contains the digital signature, which can be verified by the recipient using the sender's public key.

Digital Certificates

A digital certificate is an electronic document or container file that contains a key value and identifying information about the entity that controls the key. The certificate is often issued and certified by a third party, usually a certificate authority. Different client-server applications use different types of digital certificates to accomplish their assigned functions, as follows:

The CA application suite issues and uses certificates (keys) that identify and establish a trust relationship with a CA to determine what additional certificates (keys) can be authenticated. Mail applications use Secure/Multipurpose Internet Mail Extension (S/MIME) certificates for signing and encrypting e-mail as well as for signing forms. Development applications use object-signing certificates to identify signers of object-oriented code and scripts. Web servers and Web application servers use Secure Sockets Layer (SSL) certificates to authenticate servers via the SSL protocol

(which is described shortly) in order to establish an encrypted SSL session. Web clients use client SSL certificates to authenticate users, sign forms, and participate in single sign-on solutions via SSL.

Two popular certificate types are those created using Pretty Good Privacy (PGP) and those created using applications that conform to International Telecommunication Union's (ITU-TX.509 version 3. The X.509 v3 certificate.

It is an ITU-T recommendation that essentially defines a directory service that maintains a database (also known as a repository) of information about a group of users holding X.509 v3 certificates. An X.509 v3 certificate binds a distinguished name (DN**)**, which uniquely identifies a certificate entity, to a user's public key. The certificate is signed and placed in the directory by the CA for retrieval and verification by the user's associated public key.

Certificate structure:

Version
Certificate Serial Number
Algorithm ID
Algorithm ID
Parameters
Issuer Name
Validity
Not Before
Not After
Subject Name
Subject Public Key Info
Public Key Algorithm
Parameters
Subject Public Key
Issuer Unique Identifier (Optional)
Subject Unique Identifier (Optional)
Extensions (Optional)
Type
Criticality
Value
Certificate Signature Algorithm
Certificate Signature

Hybrid cryptography systems

The most common hybrid system is based on the Diffie-Hellman key exchange, which is a method for exchanging private keys using public key encryption. Diffie-Hellman key exchange uses asymmetric encryption to exchange **session keys**.

6. What are the seven major sources of physical loss?(Nov/Dec 2014, Nov/Dec 2012)

Seven Major Sources of Physical Loss

- Temperature extremes
- Gases
- Liquids
- Living organisms
- Projectiles
- Movement
- Energy anomalies

A secure facility is a physical location that has been engineered with controls designed to minimize the risk of attacks from physical threats

A secure facility can use the natural terrain; traffic flow, urban development, and can complement these features with protection mechanisms such as fences, gates, walls, guards, and alarms

Controls for Protecting the Secure Facility

- Walls, Fencing, and Gates
- Guards
- Dogs, ID Cards, and Badges
- Locks and Keys
- Mantraps
- Electronic Monitoring
- Alarms and Alarm Systems
- Computer Rooms
- Walls and Doors

ID Cards and Badges

- Ties physical security to information access with identification cards (ID) and/or name badges
  - ID card is typically concealed
  - Name badge is visible
- These devices are actually biometrics (facial recognition)
- Should not be the only control as they can be easily duplicated, stolen, and modified
- Tailgating occurs when unauthorized individuals follow authorized users through the control

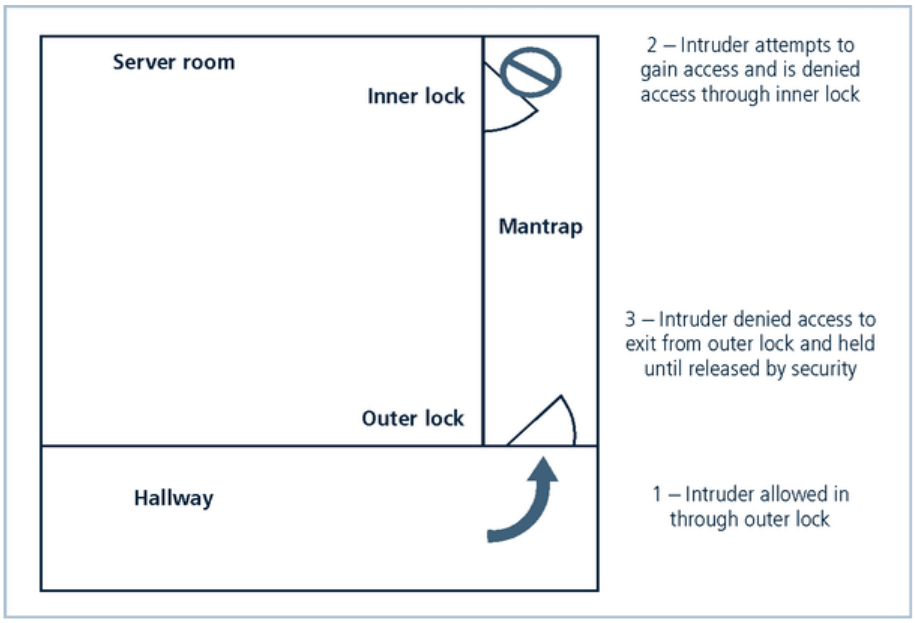
Locks and Keys

- There are two types of locks
  - mechanical and electro-mechanical
- Locks can also be divided into four categories
  - manual, programmable, electronic, and biometric
- Locks fail and facilities need alternative procedures for access
- Locks fail in one of two ways:

- when the lock of a door fails and the door becomes unlocked, that is a fail-safe lock
- when the lock of a door fails and the door remains locked, this is a fail-secure lock

Mantraps

- An enclosure that has an entry point and a different exit point
- The individual enters the mantrap, requests access, and if verified, is allowed to exit the mantrap into the facility
- If the individual is denied entry, they are not allowed to exit until a security official overrides the automatic locks of the enclosure



FIGU raps

Electroı g

- Records events where other types of physical controls are not practical
- May use cameras with video recorders
- Drawbacks:
  - reactive and do not prevent access or prohibited activity
  - recordings often not monitored in real time and must be reviewed to have any value

Alarms and Alarm Systems

- Alarm systems notify when an event occurs
- Used for fire, intrusion, environmental disturbance, or an interruption in services
- These systems rely on sensors that detect the event: motion detectors, smoke detectors, thermal detectors, glass breakage detectors, weight sensors, and contact sensors

Computer Rooms and Wiring Closets

- Computer rooms and wiring and communications closets require special attention

- Logical controls are easily defeated, if an attacker gains physical access to the computing equipment
- Custodial staff are often the least scrutinized of those who have access to offices and are given the greatest degree of unsupervised access

Interior Walls and Doors

- The walls in a facility are typically either:
    - standard interior
    - firewall
- All high-security areas must have firewall grade walls to provide physical security from potential intruders and improves the facility's resistance to fires
- Doors that allow access into secured rooms should also be evaluated
- Computer rooms and wiring closets can have push or crash bars installed to meet building codes and provide much higher levels of security than the standard door pull handle

Fire Safety

- The most serious threat to the safety of the people who work in the organization is the possibility of fire
- Fires account for more property damage, personal injury, and death than any other threat
- It is imperative that physical security plans examine and implement strong measures to detect and respond to fires and fire hazards

Fire Detection and Response

- Fire suppression systems are devices installed and maintained to detect and respond to a fire
- They work to deny an environment of one of the three requirements for a fire to burn: heat, fuel, and oxygen
    - Water and water mist systems reduce the temperature and saturate some fuels to prevent ignition
    - Carbon dioxide systems rob fire of its oxygen
    - Soda acid systems deny fire its fuel, preventing spreading
    - Gas-based systems disrupt the fire’s chemical reaction but leave enough oxygen for people to survive for a short time
    - Drafts or approves information security policies
    - Works with the CIO on strategic plans, develops tactical plans, and works with security managers on operational plans
    - Develops Information Security budgets based on funding
    - Sets priorities for Information Security projects & technology
    - Makes decisions in recruiting, hiring, and firing of security staff
    - Acts as the spokesperson for the security team