# ROHINI COLLEGE OF ENGINEERING AND TECHNOLOGY

Kanyakumari Main Road, near Anjugramam, Palkulam, Anjugramam, Tamil Nadu 629401


## DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

# ADD ON COURSE

# INFORMATION SECURITY

## COURSE MATERIAL

# INFORMATION SECURITY

## INTRODUCTION

- Information technology is the vehicle that stores and transports information—a company's most valuable resource—from one business unit to another.
- But what happens if the vehicle breaks down, even for a little while?
- As businesses have become more fluid, the concept of computer security has been replaced by the concept of information security.
- Because this new concept covers a broader range of issues, from the protection of data to the protection of human resources, information security is no longer the sole responsibility of a discrete group of people in the company; rather, it is the responsibility of every employee, and especially managers.
- Organizations must realize that information security funding and planning decisions involve more than just technical managers:
- Rather, the process should involve three distinct groups of decision makers, or communities of interest:

- Information security managers and professionals
- Information technology managers and professionals
- Nontechnical business managers and professionals

These communities of interest fulfill the following roles:

- The information security community protects the organization's information assets from the many threats they face.
- The information technology community supports the business objectives of the organization by supplying and supporting information technology appropriate to the business' needs.
- The nontechnical general business community articulates and communicates organizational policy and objectives and allocates resources to the other groups.

**WHAT IS SECURITY?**

Understanding the technical aspects of information security requires that you know the definitions of certain information technology terms and concepts.

In general, security is defined as "the quality or state of being secure—to be free from danger."

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

Specialized areas of security

- **Physical security**, which encompasses strategies to protect people, physical assets, and the workplace from various threats including fire, unauthorized access, or natural disasters
- **Personal security**, which overlaps with physical security in the protection of the people within the organization
- **Operations security**, which focuses on securing the organization's ability to carry out its operational activities without interruption or compromise
- **Communications security**, which encompasses the protection of an organization's communications media, technology, and content, and its ability to use these tools to achieve the organization's objectives
- **Network security**, which addresses the protection of an organization's data networking devices, connections, and contents, and the ability to use that network to accomplish the organization's data communication functions
- **Information security** includes the broad areas of information security management, computer and data security, and network security.

**Where it has been used?**

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

**Information Security components are**

- Confidentiality
- Integrity

- Availability(CIA)

**CIA Triangle**

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.

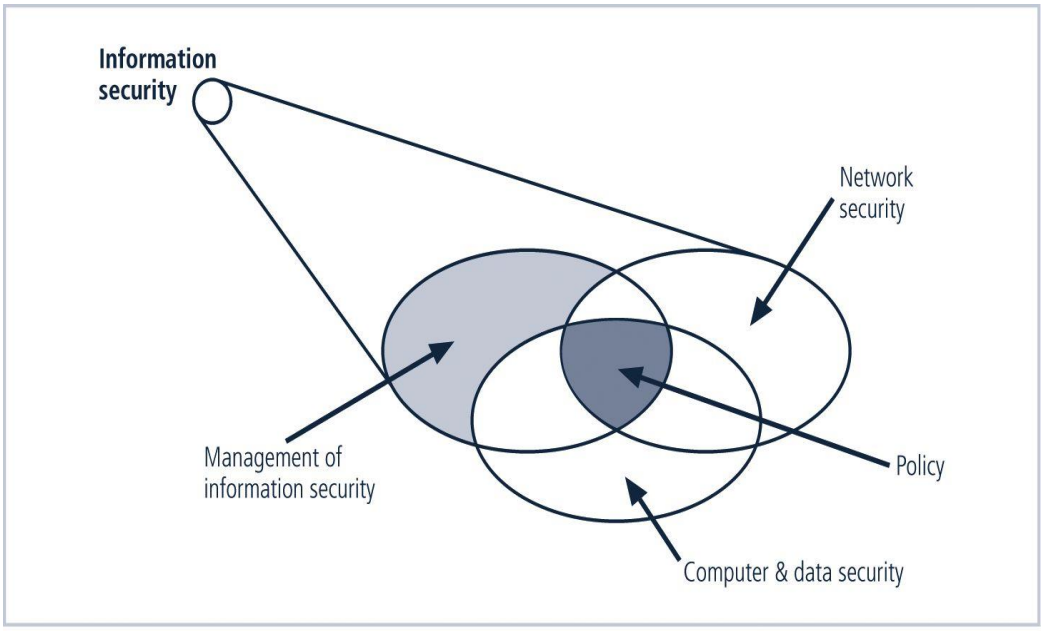



**FIGURE 1-1** Components of Information Security

**Critical Characteristics of Information**

| | | |
|---|---|---|
| -Confidentiality | - Integrity | -Availability |
| - Privacy | - Identification | - Authentication |
| - Authorization | - Accountability | -Accuracy |
| - Utility | - Possession | |

***Confidentiality***

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

- Information classification
- Secure document storage
- Application of general security policies
- Education of information custodians and end users

Example, a credit card transaction on the Internet.

- The system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the places where it might appear (in data bases, log files, backups, printed receipts, and so on), and by restricting access to the places where it is stored.
- Giving out confidential information over the telephone is a breach of confidentiality if the caller is not authorized to have the information, it could result in a breach of confidentiality.

**Integrity** Integrity is the quality or state of being whole, complete, and uncorrupted. The integrity of information is threatened when it is exposed to corruption, damage, destruction, or other disruption of its authentic state. Corruption can occur while information is being compiled, stored, or transmitted. Integrity means that data cannot be modified without authorization.

Eg: Integrity is violated when an employee deletes important data files, when a computer virus infects a computer, when an employee is able to modify his own salary in a payroll database, when an unauthorized user vandalizes a website, when someone is able to cast a very large number of votes in an online poll, and so on.

**Availability** Availability is the characteristic of information that enables user access to information without interference or obstruction and in a required format. A user in this definition may be either a person or another computer system. Availability does not imply that the information is accessible to any user; rather, it means availability to authorized users.

- For any information system to serve its purpose, the information must be available when it is needed.
- Eg: High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades.

**Privacy**

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

**Identification**

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

***Authentication***

Authentication occurs when a control provides proof that a user possesses the identity that he or she claims.

- In computing, e-Business and information security it is necessary to ensure that the data, transactions, communications or documents(electronic or physical) are genuine(i.e. they have not been forged or fabricated)

***Authorization***

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

***Accountability***

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

***Accuracy***Information should have accuracy. Information has accuracy when it is free from mistakes or errors and it has the value that the end users expects. If information contains a value

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

***Utility***

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

***Possession***

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

**NSTISSC Security Model**

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

- It is now called **the National Training Standard for Information security professionals.**

The NSTISSC Security Model provides a more detailed perspective on security.

While the NSTISSC model covers the three dimensions of information security, it omits discussion of detailed guidelines and policies that direct the implementation of controls.

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

-The 3 dimensions of each axis become a 3x3x3 cube with 27 cells representing areas that must be addressed to secure today's Information systems.

- To ensure system security, each of the 27 cells must be properly addressed during the security process.

-For ex,the intersection between technology, Integrity & storage areas requires a control or safeguard that addresses the need to use technology to protect the Integrity of information while in storage.

NSTISSC Security Model

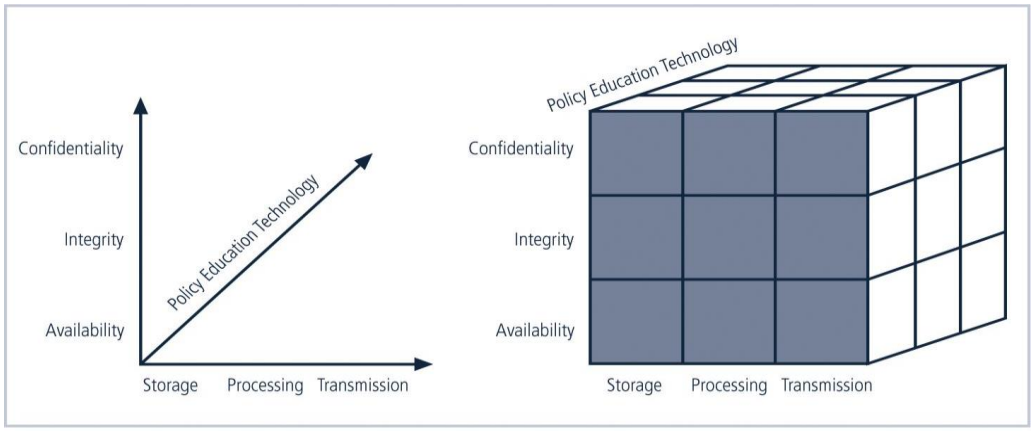



**FIGURE 1-2** NSTISSC Security Model

## Components of an Information System

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

### Software

The software components of IS comprises applications, operating systems, and assorted command utilities. Software programs are the vessels that carry the lifeblood of information through an organization. These are often created under the demanding constraints of project management, which limit time, cost, and manpower.

### Hardware

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

**Data**

- Data stored, processed, and transmitted through a computer system must be protected.
- Data is often the most valuable asset possessed by an organization and is the main target of intentional attacks.
- The raw, unorganized, discrete(separate, isolated) potentially-useful facts and figures that are later processed(manipulated) to produce information.

**People**

There are many roles for people in information systems. Common ones include

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

**Procedures**

A procedure is a series of documented actions taken to achieve something. A procedure is more than a single simple task. A procedure can be quite complex and involved, such as performing a backup, shutting down a system, patching software.

**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.

***Securing Components***

-Protecting the components from potential misuse and abuse by unauthorized users.

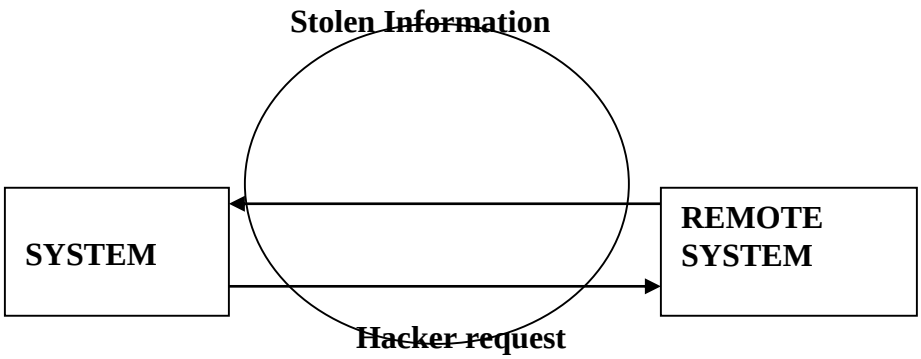
**Subject of an attack –** Computer is used as an active tool to conduct the attack.

**Object of an attack –** Computer itself is the entity being attacked

.**Two types of attacks**

**- Direct attack**

***- Indirect***




Hacker using a computer as the subject of attack

Remote system that is the object of an attack

1. **Direct attack**

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

2. **Indirect attack**

When a system is compromised and used to attack other system.

[Originate from a system or resource that itself has been attacked, and is malfunctioning or working under the control of a threat].

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

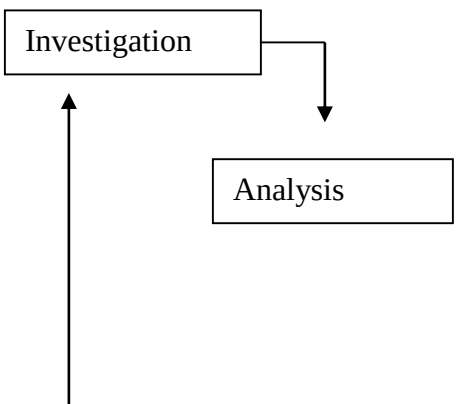
**Balancing Information Security and Access**

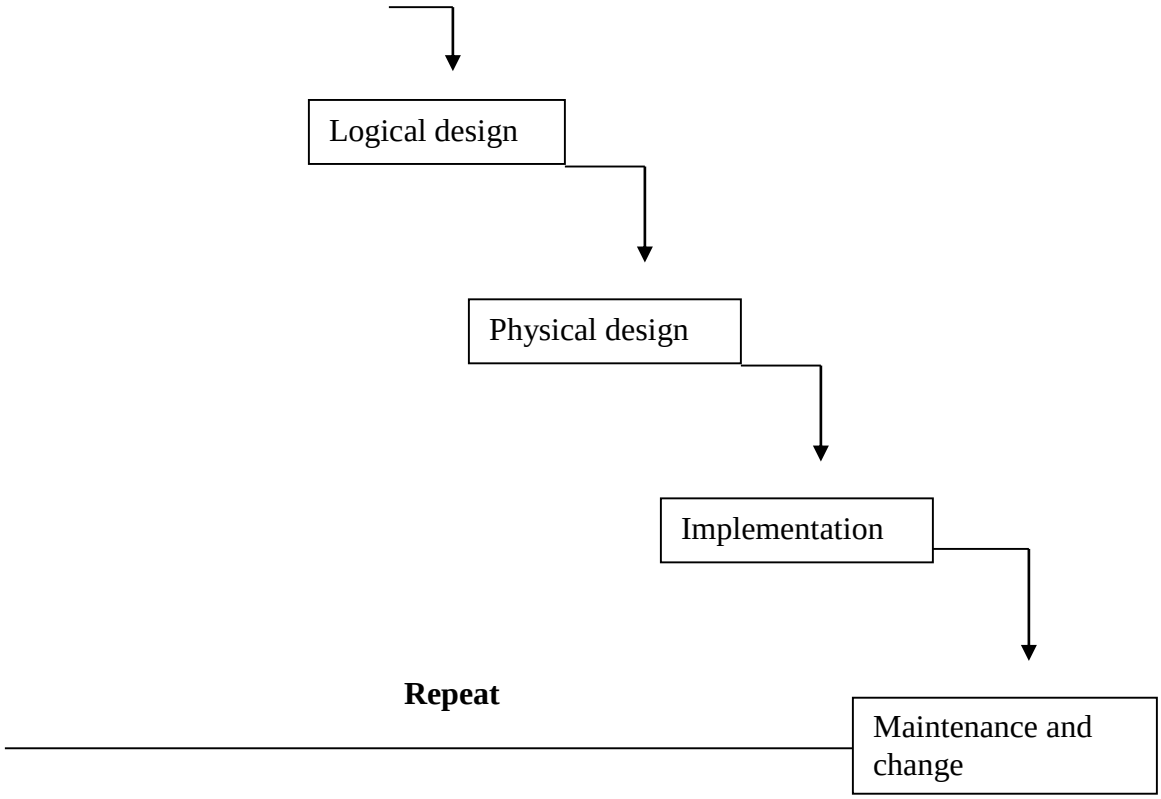
- Has to provide the security and is also feasible to access the information for its application.
- Information Security cannot be an absolute: it is a process, not a goal.
- Should balance protection and availability.

**Approaches to Information Security Implementation**

- Bottom- up- approach.
- Top-down-approach
  - ➔ Has higher probability of success.
  - ➔ Project is initiated by upper level managers who issue policy & procedures & processes.
  - ➔ Dictate the goals & expected outcomes of the project.
  - ➔ Determine who is suitable for each of the required action.

**The Systems Development Life Cycle (SDLC)**






**SDLC Waterfall Methodology**

**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.
- SDLC consists of 6 phases.

**Investigation**

- It is the most important phase and it begins with an examination of the event or plan that initiates the process.
- During this phase, the objectives, constraints, and scope of the project are specified.
- At the conclusion of this phase, a feasibility analysis is performed, which assesses the economic, technical and behavioral feasibilities of the process and ensures that implementation is worth the organization's time and effort.

**Analysis**

- It begins with the information gained during the investigation phase.

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

**Logical Design**

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

**Physical design**

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

**Implementation**

- In this phase, any needed software is created.
- Components are ordered, received and tested.
- Afterwards, users are trained and supporting documentation created.
- Once all the components are tested individually, they are installed and tested as a system.

- Again a feasibility analysis is prepared, and the sponsors are then presented with the system for a performance review and acceptance test.

**Maintenance and change**

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

**The Security Systems Development Life Cycle (Sec SDLC )**

- The same phases used in the traditional SDLC can be adapted to support the implementation of an information security project.

**Investigation**

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

**Analysis**

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

- The developed team conducts a preliminary analysis of existing security policies or programs, along with that of documented current threats and associated controls.
- The risk management task also begins in this phase.

-**Risk management** is the process of identifying, assessing, and evaluating the levels of risk facing the organization, specifically the threats to the organization's security and to the information stored and processed by the organization.

**Logical design**

- This phase creates and develops the blueprints for information security, and examines and implements key policies.
- The team plans the incident response actions.
- Plans business response to disaster.
- Determines feasibility of continuing and outsourcing the project.

**Physical design**

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

**Implementation**

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

**Maintenance and change**

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

**<u>Security Professionals and the organization</u>**

**Senior management**

Chief information Officer (CIO) is the responsible for

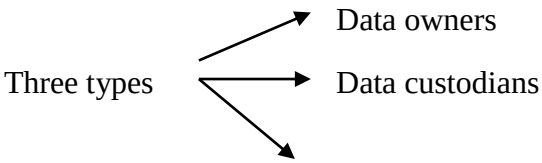
- ➔ Assessment
- ➔ Management
- ➔ And implementation of information security in the organization

**Information Security Project Team**

- **Champion**
  - Promotes the project
  - Ensures its support, both financially & administratively.
- **Team Leader**
  - Understands project management
  - Personnel management
  - And information Security technical requirements.
- **Security policy developers**
  - individuals who understand the organizational culture,
  - existing policies
  - Requirements for developing & implementing successful policies.
- **Risk assessment specialists**
  - Individuals who understand financial risk assessment techniques.
  - The value of organizational assets,
  - and the security methods to be used.
- **Security Professionals**
  - Dedicated

- Trained, and well educated specialists in all aspects of information security from both a technical and non technical stand point.

- **System Administrators**
  - Administrating the systems that house the information used by the organization.
- **End users**




**Data Owners**

- Responsible for the security and use of a particular set of information.
- Determine the level of data classification
- Work with subordinate managers to oversee the day-to-day administration of the data.

**Data Custodians**

- Responsible for the storage, maintenance, and protection of the information.
- Overseeing data storage and backups
- Implementing the specific procedures and policies.

**Data Users (End users)**

- Work with the information to perform their daily jobs supporting the mission of the organization.
- Everyone in the organization is responsible for the security of data, so data users are included here as individuals with an information security role.

**<u>Key Terms in Information Security Terminology</u>**

**Asset**

-An asset is the organizational resource that is being protected.

-An Asset can be logical, such as

Website, information or data

- Asset can be physical, such as

➔ person , computer system

**Attack**

- An attack is an intentional or unintentional attempt to cause damage to or otherwise compromise the information and /or the systems that support it. If someone casually reads sensitive information not intended for his use, this is considered a passive attack. If a hacker attempts to break into an information system, the attack is considered active.

**Risk**

- Risk is the probability that something can happen. In information security, it could be the probability of a threat to a system.

**Security Blueprint**

- It is the plan for the implementation of new security measures in the organization. Sometimes called a frame work, the blueprint presents an organized approach to the security planning process.

**Security Model**

- A security model is a collection of specific security rules that represents the implementation of a security policy.

**Threats**

-A threat is a category of objects, persons, or other entities that pose a potential danger to an asset. Threats are always present. Some threats manifest themselves in accidental occurrences, while others are purposeful. For example, all hackers represent potential danger or threat to an unprotected information system. Severe storms are also a threat to buildings and their contents.

**Threat agent**

- A threat agent is the specific instance or component of a threat. For example, you can think of all hackers in the world as a collective threat, and Kevin Mitnick, who was convicted for hacking into phone systems, as a specific threat agent. Likewise, a specific lightning strike, hailstorm, or tornado is a threat agent that is part of the threat of severe storms.

**Vulnerability**

- Weaknesses or faults in a system or protection mechanism that expose information to attack or damage are known as vulnerabilities. Vulnerabilities that have been examined, documented, and published are referred to as **well-known vulnerabilities.**

**Exposure**

- The exposure of an information system is a single instance when the system is open to damage. Vulnerabilities can cause an exposure to potential damage or attack from a threat. Total exposure is the degree to which an organization's assets are at risk of attack from a threat..

## SECURITY INVESTIGATION

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

**2.1Business Needs First**

Information security performs four important functions for an organization:

1. Protects the organization's ability to function
2. Enables the safe operation of applications implemented on the organization's IT systems.
3. Protects the data the organization collects and uses.
4. Safeguards the technology assets in use at the organization.

**1. Protecting the functionality of an organization**

- Decision makers in organizations must set policy and operate their organizations in compliance with the complex, shifting legislation that controls the use of technology.

**2. Enabling the safe operation of applications**

- Organizations are under immense pressure to acquire and operate integrated, efficient, and capable applications
- The modern organization needs to create an environment that safeguards applications using the organization's IT systems, particularly those applications that serve as important elements of the infrastructure of the organization.

**3. Protecting data that organizations collect & use**

- Protecting data in motion
- Protecting data at rest
- Both are critical aspects of information security.
- The value of data motivates attackers to seal, sabotage, or corrupt it.
- It is essential for the protection of integrity and value of the organization's data

**4. Safeguarding Technology assets in organizations**

- Must add secure infrastructure services based on the size and scope of the enterprise.
- Organizational growth could lead to the need for **public key infrastructure,** PKI, an integrated system of software, encryption methodologies.

## 2.2 THREATS

To protect an organization's information, you must

1. Know yourself

(i.e) 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.

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

**Threats to Information Security**

| Categories of threat | | Examples |
|---|---|---|
| 1).Acts of human error or failure | -- | Accidents, employee mistakes |
| 2).Compromises to intellectual property | -- | Piracy, copyright infringement |
| 3).Deliberate acts of espionage or trespass | -- | Unauthorized access and/or/data collection |
| 4).Deliberate acts of information extortion | -- | Blackmail or information disclosure |
| 5).Deliberate acts of sabotage or vandalism | -- | Destruction of systems or information |
| 6).Deliberate acts of theft | -- | Illegal confiscation of equipment or information |

7).Deliberate software attacks -- Viruses, worms, macros, denial-of-service

8).Forces of nature -- Fire, flood, earthquake, lightning

9).Deviations in quality of service -- ISP, power ,or WAN service providers

10).Technical hardware failures or errors -- Equipment failure

11).Technical software failures or errors -- Bugs, code problems, unknown loopholes

12).Technological obsolescence -- Antiquated or outdated technologies

**Threats**

**1. Acts of Human Error or Failure:**

- Acts performed without intent or malicious purpose by an authorized user.
- because of in experience , improper training,
- Making of incorrect assumptions.

One of the greatest threats to an organization's information security is the organization's own employees.

- Entry of erroneous data
- accidental deletion or modification of data
- storage of data in unprotected areas.
- Failure to protect information

can be prevented with

- Training

- Ongoing awareness activities

-Verification by a second party

- Many military applications have robust, dual- approval controls built in .

**2. Compromises to Intellectual Property**

- 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.

2. Software and Information Industry Association (SIIA)
   (i.e)Software Publishers Association
3. Business Software Alliance (BSA)
    - Another effort to combat (take action against) piracy is the online registration process.

**3. Deliberate Acts of Espionage or Trespass**

- Electronic and human activities that can breach the confidentiality of information.
- When an unauthorized individual's gain access to the information an organization is trying to protect is categorized as act of espionage or trespass.
- Attackers can use many different methods to access the information stored in an information system.

1. Competitive Intelligence[use web browser to get information from market research]
2. Industrial espionage(spying)
3. Shoulder Surfing(ATM)

**Trespass**

- Can lead to unauthorized real or virtual actions that enable information gatherers to enter premises or systems they have not been authorized to enter.
- 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**

- Destroy an asset or
- 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.
- Trained security professionals.
- Electronic theft control is under research.

**7. Deliberate Software Attacks**

- Because of **malicious code** or **malicious software** or sometimes **malware.**
- These software components are designed to damage, destroy or deny service to the target system.
- More common instances are

  Virus, Worms, Trojan horses, Logic bombs, Backdoors.
- "The British Internet Service Provider Cloudnine" be the first business "hacked out of existence"

**Virus**

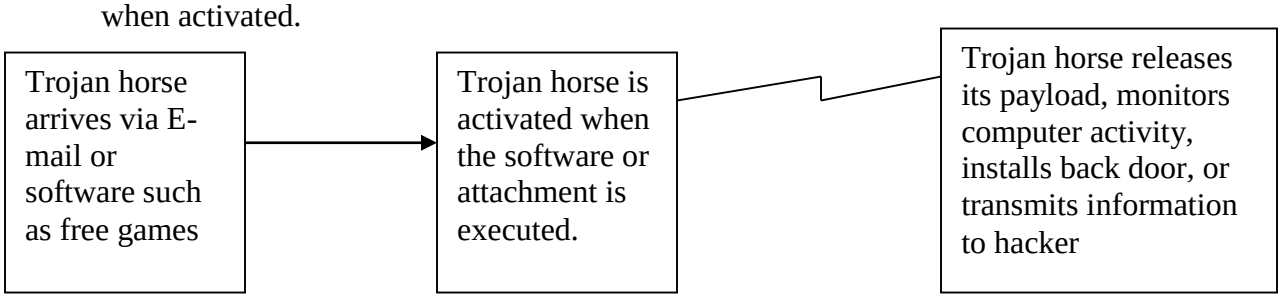
- Segments of code that performs malicious actions.
- Virus transmission is at the opening of Email attachment files.
- **Macro virus**-> Embedded in automatically executing macrocode common in word processors, spreadsheets and database applications.
- **Boot Virus**-> infects the key operating files located in the computer's boot sector.

**Worms**A worm is a malicious program that replicates itself constantly, without requiring another program to provide a safe environment for replication.

- Worms can continue replicating themselves until they completely fill available resources, such as memory, hard drive space, and network bandwidth.
- Eg: MS-Blaster, MyDoom, Netsky, are multifaceted attack worms.
- 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 systems can reach, so that users who subsequently visit those sites become infected.

**Trojan Horses**

- Are software programs that hide their true nature and reveal their designed behavior only when activated.




**Trojan horse Attack**

**Back Door or Trap Door**

- A Virus or Worm has a payload that installs a backdoor or trapdoor component in a system, which allows the attacker to access the system at will with special privileges.

Eg: Back Orifice

**Polymorphism**

- A **Polymorphic threat** is one that changes its apparent shape over time, making it undetectable by techniques that look for preconfigured signatures.
- These viruses and Worms actually evolve, changing their size, and appearance to elude detection by antivirus software programs.

**Virus & Worm Hoaxes**

**<u>Types of Trojans</u>**

- Data Sending Trojans

- Proxy Trojans
- FTP Trojans
- Security software disabler Trojans
- Denial of service attack Trojans(DOS)

**Virus**

A program or piece of code that be loaded on to your computer, without your knowledge and run against your wishes.

**Worm**

A program or algorithm that replicates itself over a computer network and usually performs malicious actions.

**Trojan Horse**

A destructive program that masquerade on beginning application, unlike viruses, Trojan horse do not replicate themselves.

**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.

**8)Forces of Nature**

**Fire:** Structural fire that damages the building. Also encompasses smoke damage from a fire or water damage from sprinkles systems.

**Flood:** Can sometimes be mitigated with flood insurance and/or business interruption Insurance.

**Earthquake:** Can sometimes be mitigated with specific causality insurance and/or business interruption insurance, but is usually a separate policy.

**Lightning**: An Abrupt, discontinuous natural electric discharge in the atmosphere.

**Landslide/Mudslide**: The downward sliding of a mass of earth & rocks directly damaging all parts of the information systems.

**Tornado/Severe Windstorm:**

**Huricane/typhoon:**

**Tsunami:**

**Electrostatic Discharge (ESD):**

**Dust Contamination:**

Since it is not possible to avoid force of nature threats, organizations must implement controls to limit damage.

- They must also prepare contingency plans for continued operations, such as disaster recovery plans, business continuity plans, and incident response plans, to limit losses in the face of these threats.

**9) Deviations in Quality of Service**

- A product or service is not delivered to the organization as expected.
- The Organization's information system depends on the successful operation of many interdependent support systems.
- It includes power grids, telecom networks, parts suppliers, service vendors, and even the janitorial staff & garbage haulers.
- This degradation of service is a form of **availability disruption.**

**Internet Service Issues**

- Internet service Provider(ISP) failures can considerably undermine the availability of information.
- The web hosting services are usually arranged with an agreement providing minimum service levels known as a **Service level Agreement (SLA).**
- When a Service Provider fails to meet SLA, the provider may accrue fines to cover losses incurred by the client, but these payments seldom cover the losses generated by the outage.

**Communications & Other Service Provider Issues**

- Other utility services can affect the organizations are telephone, water, waste water, trash pickup, cable television, natural or propane gas, and custodial services.
- The loss of these services can impair the ability of an organization to function.
- For an example, if the waste water system fails, an organization might be prevented from allowing employees into the building.
- This would stop normal business operations.

**Power Irregularities**

- Fluctuations due to power excesses.
- Power shortages &
- Power losses

This can pose problems for organizations that provide inadequately conditioned power for their information systems equipment.

- When voltage levels **spike** (experience a momentary increase),or **surge** ( experience prolonged increase ), the extra voltage can severely damage or destroy equipment.
- The more expensive uninterruptible power supply (UPS) can protect against spikes and surges.

**Technical Hardware Failures or Errors**

- Resulting in unreliable service or lack of availability
- Some errors are terminal, in that they result in unrecoverable loss of equipment.
- Some errors are intermittent, in that they resulting in faults that are not easily repeated.

**Technical software failures or errors**

- This category involves threats that come from purchasing software with unknown, hidden faults.
- Large quantities of computer code are written, debugged, published, and sold before all their bugs are detected and resolved.
- These failures range from bugs to untested failure conditions.

**Technological obsolescence**

- Outdated infrastructure can lead to unreliable and untrustworthy systems.
- Management must recognize that when technology becomes outdated, there is a risk of loss of data integrity from attacks.

## 2.3 ATTACKS

- An attack is an act of or action that takes advantage of a vulnerability to compromise a controlled system.
- It is accomplished by a **threat agent** that damages or steals an organization's information or physical asset.

- **Vulnerability** is an identified weakness in a controlled system, where controls are not present or are no longer effective.
- Attacks exist when a specific act or action comes into play and may cause a potential loss.

**Malicious code**

- The malicious code attack includes the execution of viruses, worms, Trojan horses, and active Web scripts with the intent to destroy or steal information.
- The state –of-the-art malicious code attack is the polymorphic or multivector, worm.
- These attack programs use up to six known attack vectors to exploit a variety of vulnerabilities in commonly found information system devices.

**Attack Replication Vectors**

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

**1. IP scan & attack**

The infected system scans a random or local range of IP addresses and targets any of several vulnerabilities known to hackers.

**2. Web browsing**

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

**3. Virus**

Each infected machine infects certain common executable or script files on all computers to which it can write with virus code that can cause infection.

**4. Unprotected shares**

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

**5. Mass Mail**

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

**6. Simple Network Management Protocol (SNMP)**

- By using the widely known and common passwords that were employed in early versions of this protocol, the attacking program can gain control of the device. Most vendors have closed these vulnerabilities with software upgrades.

**Hoaxes**

- A more devious approach to attacking the computer systems is the transmission of a virus hoax with a real virus attached.
- Even though these users are trying to avoid infection, they end up sending the attack on to their co-workers.

**Backdoors**

- Using a known or previously unknown and newly discovered access mechanism, an attacker can gain access to a system or network resource through a back door.
- Sometimes these entries are left behind by system designers or maintenance staff, and thus referred to as trap doors.
- A trap door is hard to detect, because very often the programmer who puts it in place also makes the access exempt from the usual audit logging features of the system.

**Password Crack**

- Attempting to reverse calculate a password is often called **cracking.**
- A password can be hashed using the same algorithm and compared to the hashed results, If they are same, the password has been cracked.
- The (SAM) Security Account Manager file contains the hashed representation of the user's password.

**Brute Force**

- The application of computing & 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.**

**Dictionary**

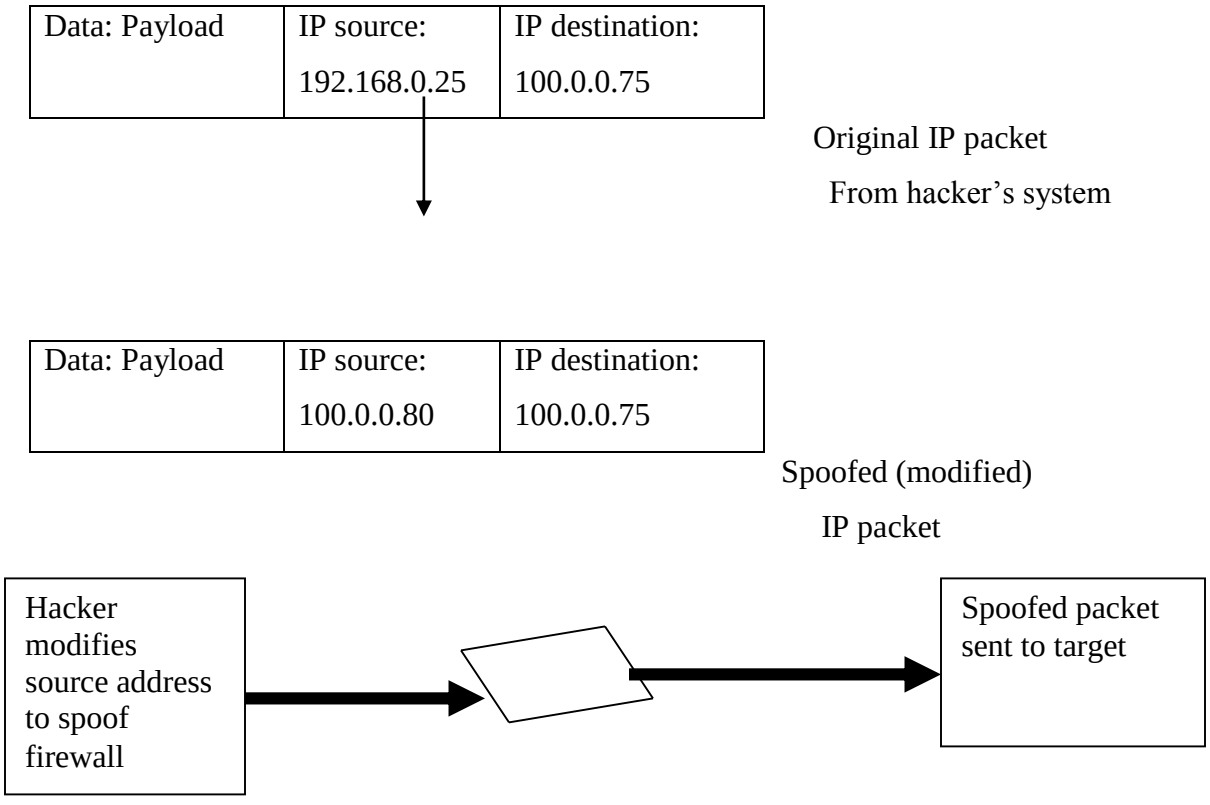
- This is another form of the brute force attack noted above for guessing passwords.
- The **dictionary attack** narrows the field by selecting specific accounts to attack and uses a list of commonly used passwords instead of random combinations.

**Denial –of- Services(DOS) & Distributed Denial –of- Service(DDOS)**

- The attacker sends a large number of connection or information requests to a target.
- This may result in the system crashing, or simply becoming unable to perform ordinary functions.
- DDOS is an attack in which a coordinated stream of requests is launched dagainst a target from many locations at the same.

**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.



Firewall allows packet in, mistaking it for intimate traffic

## IP spoofing

### Man-in-the –Middle

- Otherwise called as **TCP hijacking attack**.
- An attacker monitors packets from the network, modifies them, and inserts them back into the network.
- This type of attack uses IP spoofing.
- It allows the attacker to change, delete, reroute, add, forge or divert data.
- TCP hijacking session, the spoofing involves the interception of an encryption key exchange.

### SPAM

- Spam is unsolicited commercial E-mail.
- It has been used to make malicious code attacks more effective.
- Spam is considered as a trivial nuisance rather than an attack.
- It is the waste of both computer and human resources it causes by the flow of unwanted E-mail.

### Mail Bombing

- Another form of E-mail attack that is also a DOS called a **mail bomb**.
- Attacker routes large quantities of e-mail to the target.
- The target of the attack receives unmanageably large volumes of unsolicited e-mail.
- By sending large e-mails, attackers can take advantage of poorly configured e-mail systems on the Internet and trick them into sending many e-mails to an address chosen by the attacker.
- The target e-mail address is buried under thousands or even millions of unwanted e-mails.

### Sniffers

- A **sniffer** is a program or device that can monitor data traveling over 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.

- Sniffer often works on TCP/IP networks, where they are sometimes called **"packet Sniffers".**

**Social Engineering**

- It is the process of using social skills to convince people to reveal access credentials or other valuable information to the attacker.
- An attacker gets more information by calling others in the company and asserting his/her authority by mentioning chief's name.

**Buffer Overflow**

- A buffer overflow is an application error that occurs when more data is sent to a buffer than it can handle.
- Attacker can make the target system execute instructions.
- This buffer overflow could results in denial of service attack.

**Timing Attack**

- Works by exploring the contents of a web browser's cache.
- These attacks allow a Web designer to create a malicious form of cookie, that is stored on the client's system.
- The cookie could allow the designer to collect information on how to access password-protected sites.

**LEGAL, ETHICAL, AND PROFESSIONAL ISSUES IN INFORMATION SECURITY**

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.**

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

| ACT | SUBJECT | DATE | DESCRIPTION |
|---|---|---|---|

| | | | |
|---|---|---|---|
| Communications Act of 1934,updated by Telecommunications Deregulation & Competition Act | Telecommunications | 1934 | Regulates interstate and foreign Telecommunications. |
| Computer Fraud & Abuse Act | Threats to computers | 1986 | Defines and formalizes laws to counter threats from computer related acts and offenses. |
| Computer Security Act of 1987 | Federal Agency Information Security | 1987 | Requires all federal computer systems that contain classified information to have surety plans in place, and requires periodic security training for all individuals who operate, design, or manage such systems. |
| Economic Espionage Act of 1996 | Trade secrets. | 1996 | Designed to prevent abuse of information gained by an individual working in one company and employed by another. |
| Electronic Communications Privacy Act of 1986 | Cryptography | 1986 | Also referred to as the Federal Wiretapping Act; regulates interception and disclosure of electronic information. |
| Federal Privacy Act of 1974 | Privacy | 1974 | Governs federal agency use of personal information. |

| | | | |
|---|---|---|---|
| Gramm-Leach-Bliley Act of 1999 | Banking | 1999 | Focuses on facilitating affiliation among banks, insurance and securities firms; it has significant impact on the privacy of personal information used by these industries. |
| Health Insurance Portability and Accountability Act | Health care privacy | 1996 | Regulates collection, storage, and transmission of sensitive personal health care information. |
| National Information Infrastructure protection Act of 1996 | Criminal intent | 1996 | Categorized crimes based on defendant's authority to access computer and criminal intent. |
| Sarbanes-Oxley Act of 2002 | Financial Reporting | 2002 | Affects how public organizations and accounting firms deal with corporate governance, financial disclosure, and the practice of public accounting. |
| Security and Freedom through Encryption Act of 1999 | Use and sale of software that uses or enables encryption. | 1999 | Clarifies use of encryption for people in the United states and permits all persons in the U.S. to buy or sell any encryption product and states that the government cannot require the use of any kind of key |

| | | | |
|---|---|---|---|
| | | | escrow system for encryption products. |
| U.S.A. Patriot Act of 2001 | Terrorism | 2001 | Defines stiffer penalties for prosecution of terrorist crimes. |

## SECURITY ANALYSIS

## RISK MANAGEMENT

**Definition:**

The formal process of identifying and controlling the risks facing an organization is called risk management. It is the probability of an undesired event causing damage to an asset. There are three steps

1. Risk Identification.
2. Risk Assessment
3. Risk Control

**Risk Identification**: It is the process of examining and documenting the security posture of an organization's information technology and the risk it faces.

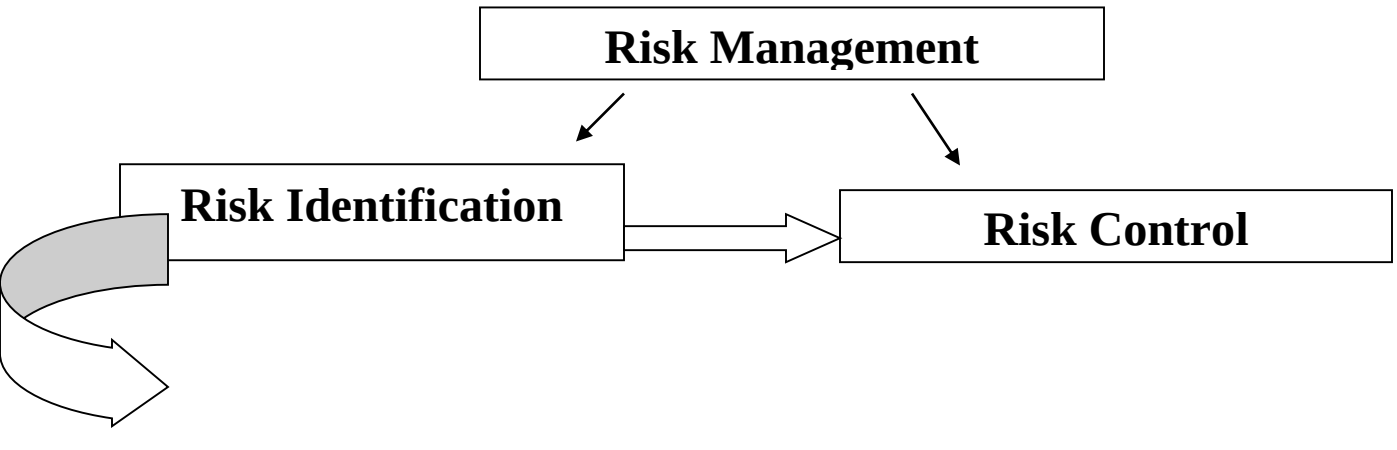
**Risk Assessment**: It is the documentation of the results of risk identification.

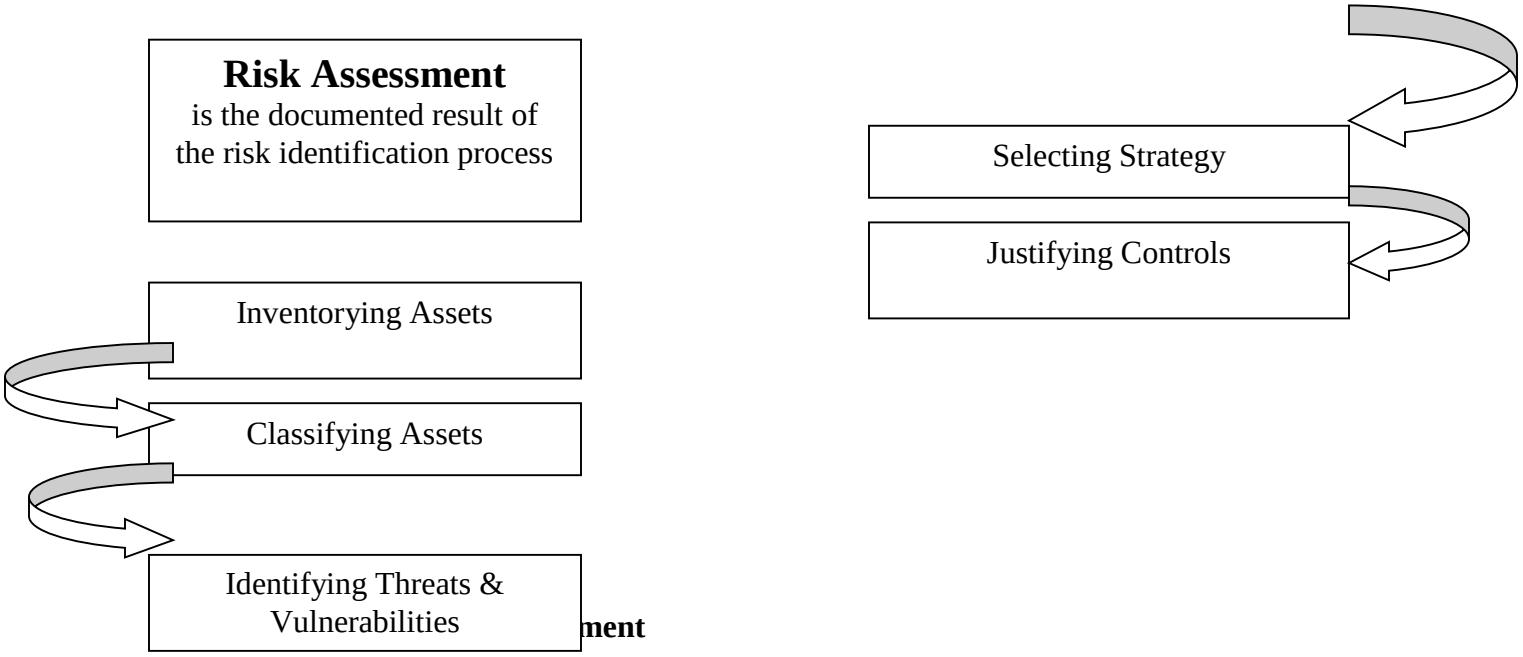
**Risk Control**: It is the process of applying controls to reduce the risks to an organization's data and information systems.

To keep up with the competition, organizations must design and create safe environments in which business process and procedures can function.

These environments must maintain Confidentiality & Privacy and assure the integrity of organizational data-objectives that are met through the application of the principles of risk management

**Components of Risk Management**






**ment**

Over 2,400 years ago by Chinese General Sun Tzu said

"1.If you know the enemy & know yourself, you need not fear the result of a hundred battles.

2. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.

3. If you know neither the enemy nor yourself, you will succumb in every battle"

**Know Yourself**

- Identify, Examine & Understand the information systems.
- To protect assets, you must understand what they are? How they add value to the organization, and to which vulnerabilities they are susceptible.
- The policies, Education and training programs, and technologies that protect information must be carefully maintained and administered to ensure that they are still effective.

**Know the Enemy**

- Identifying, Examining & Understanding the threats facing the organization.
- Among those threats,the potential and dierect threats must be identified and proper safeguards must be implemented to protect the organizational assets.
- The risks may be **internal** or **external**
- Those risks that come from risk factors within the organization are called **internal** risks whereas the **external risks** come from out of the organization and are difficult to control

**The Roles of the Communities of Interest**

- It is the responsibility of each community of interest to manage the risks that organization encounters.

**Information Security**

- Understand the threats and attacks that introduce risk into the organization.
- They take a leadership role in designing security programs and administering this within the organization.

**Management & Users**

- Management must ensure that sufficient resource are allocated to the information security & Information technology groups to meet the security needs of the organization.
- Users work with the systems and the data and are therefore well positioned to understand the value of the information assets.
- They are the people who face the security threats at the stages.

**Information Technology**

- Must build secure systems and operate them safely.

Three communities of interest are also responsible for the following

- Evaluating the risk controls.
- Determining which control options are cost effective.
- Acquiring or installing the needed controls.
- Overseeing that the controls remain effective.

**Important Risk Factors of information Security are**

i. Understand the threats and attacks that introduce risk into the organization.
ii. Taking asset inventory.
iii. Verify the threats and vulnerabilities that have been identified as dangerous to the asset inventory, as well as the current controls and mitigation strategies.
iv. Review the cost effectiveness of various risk control measures.

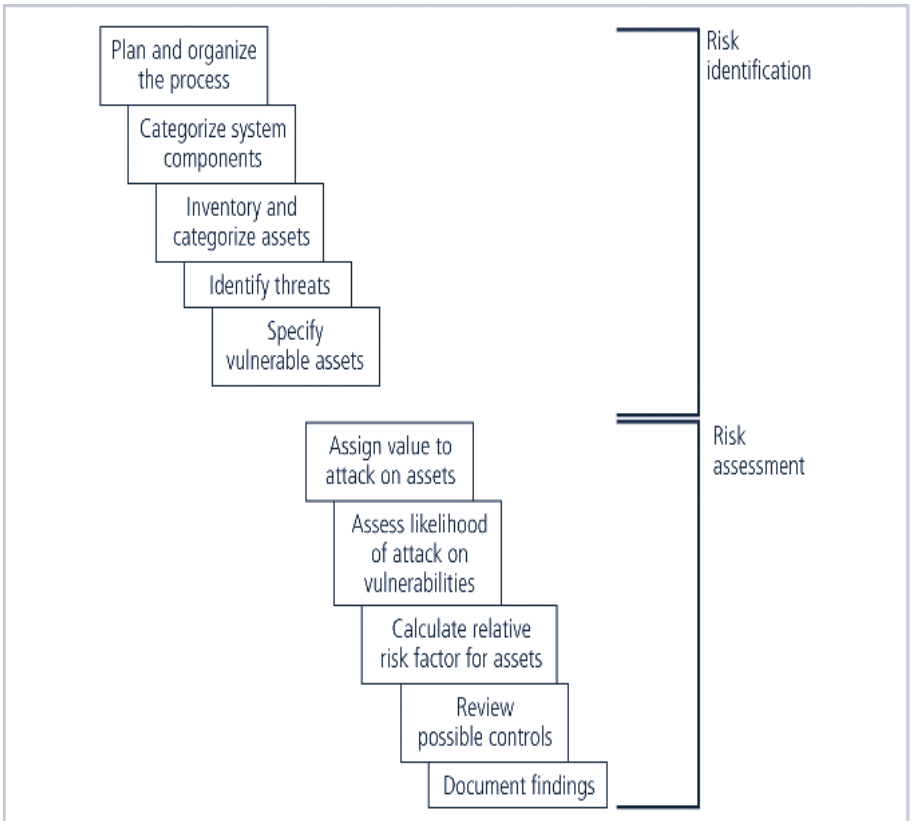
**IDENTIFYING RISKS**

- IT professionals to 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.

- Once the organizational assets have been identified, a threat identification process is undertaken.
- The circumstances and settings of each information asset are examined to identify vulnerabilities.
- When vulnerabilities are found, controls are identified and assessed as to their capability to limit possible losses in the eventuality of attack.
- The process of Risk Identification begins with the identification of the organization's information assets and an assessment of their value.
- The Components of this process are shown in figure

**Asset Identification & Valuation**

- Includes all the elements of an organization's system, such as people, procedures, data and information, software, hardware, and networking elements.
- Then, you classify and categorize the assets, adding details.



# Components of Risk Identification

## Categorization of IT Components

| Traditional system components | SecSDLC and risk management system components | |
|---|---|---|
| People | Employees | Trusted employees<br>Other staff |
| | Nonemployees | People at trusted organizations<br>Strangers |
| Procedures | Procedures | IT and business standard procedures<br>IT and business sensitive procedures |
| Data | Information | Transmission<br>Processing<br>Storage |
| Software | Software | Applications<br>Operating systems<br>Security components |
| Hardware | System devices and peripherals | Systems and peripherals<br>Security devices |
| | Networking components | Intranet components<br>Internet or DMZ components |

- **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. Nonemployees include contractors and consultants, members of other organizations with which the organization has a trust relationship, and strangers.

- **Procedures** fall into two categories: IT and business standard procedures, and IT and business sensitive procedures. The business sensitive procedures are those that may assist a threat agent in crafting an attack against the organization or that have some other content or feature that may introduce risk to the organization.

- **Data** Components have been expanded to account for the management of information in all stages: Transmission, Processing, and Storage.

- **Software Components** can be assigned to one of three categories: Applications, Operating Systems, or security components. Software Components that provide security controls may span the range of operating systems and applications categories, but are differentiated by the fact that they are the part of the information security control environment and must be protected more thoroughly than other system 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**

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
        - Device class= S (Server)
        - Device OS= W2K ( Windows 2000)
        - 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. An FCO is an authorization issued by an organization for the repair, modification, or update of a piece of equipment. Documenting the revision number and FCO is particularly important for networking devices that function mainly through the software running on them. For example, firewall devices often have three versions: an operating

system (OS) version, a software version, and a basic input/output system (BIOS) firmware version.

- **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.

**Automated Risk Management Tools**

-Automated tools identify the system elements that make up the hardware, software, & network components.

-Many organizations use automated asset inventory systems.

-The inventory listing is usually available in a data base.

- Once stored, the inventory listing must be kept current, often by means of a tool that periodically refreshes the data.

**Information Asset Classification**-

The data or information is further classified as

- Confidential data
- Internal data
- Public data

Another dimension of data is personnel security clearance which identifies the level of information each individual is authorized to know

- **Comprehensive:** All the information asset should finds its place in some category
- **Mutually exclusive**: Any information asset should be in only one category

**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.

-Weighting criteria is used to evaluate each information asset.

Before beginning the inventory process, the organization should determine which criteria can best be used to establish the value of the information assets. Among the criteria to be considered are:

- 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 probability?
- Which Information asset would be the expensive to replace?

**Sample Inventory 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 |

**Weighting factor analysis** is one of the ways to order or prioritize the assets

**Data Classification**

According to Georgia Pacific Corporation data is classified into three categories:

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.

**US military classification** scheme 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.

**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**

- 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.
- A 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→** 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.

## Identify and Prioritize Threats and Threat Agents

### Threats to Information Security

| Threat | Example |
|---|---|
| Act of human error or failure | Accidents, employee mistakes |
| Compromises to intellectual property | Piracy, copyright infringement |
| Deliberate acts of espionage or trespass | Unauthorized access and data collection |
| Deliberate acts of information extortion | Blackmail for information disclosure |
| Deliberate acts of sabotage or vandalism | Destruction of systems or information |
| Deliberate acts of theft | Illegal confiscation of equipment or information |
| Deliberate software attacks | Viruses, worms, macros, denial of service |
| Forces of nature | Fire, flood, earthquake, lightning |
| Quality of service deviations from service providers | Power and WAN quality of service issues |
| Technical hardware failures or errors | Equipment failure |
| Technical software failures or errors | Bugs, code problems, unknown loopholes |
| Technological obsolescence | Antiquated or outdated technologies |

- This examination is known as a threat assessment. You can address each threat with a few basic questions, as follows:
- 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?

**Weighted Ranks of Threats to Information Security**

| Threat | Mean | Standard Deviation | Weight | Weighted Rank |
|---|---|---|---|---|
| Deliberate software attacks | 3.99 | 1.03 | 546 | 2178.3 |
| Forces of Nature | 2.80 | 1.09 | 218 | 610.9 |
| Acts of human error or failure | 3.15 | 1.11 | 350 | 1101.0 |
| Deliberate acts of theft | 3.07 | 1.30 | 226 | 694.5 |
| Technological obsolescence | 2.71 | 1.11 | 158 | 427.9 |
| Technical software failures or errors | 3.16 | 1.13 | 358 | 1129.9 |
| Compromises to intellectual property | 2.72 | 1.21 | 181 | 494.8 |

**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.

**Vulnerability Assessment of a Hypothetical DMZ Router**

| Threat | Possible Vulnerabilities |
|---|---|
| Deliberate software attacks | Internet protocol is vulnerable to denial of service. |
| Acts of human error or failure | Employees may cause outage if configuration errors are made. |
| Technical software failures or errors | Vendor-supplied routing software could fail and cause an outage. |
| Technical hardware failures or errors | Hardware can fail and cause an outage. |
| Deviations in Quality of service | Power system failures are always possible. |
| Deliberate acts of sabotage or vandalism | Internet protocol is vulnerable to denial of service. |

| | |
|---|---|
| Deliberate acts of theft | This information asset has little intrinsic value, but other assets protected by this device could be attacked if it is compromised. |
| Technological obsolescence | If this asset is not reviewed and periodically updated, it may fall too far behind its vendor support model to be kept in service. |
| Forces of nature | All information assets in the organization are subject to forces of nature, unless suitable controls are provided. |
| Compromises to intellectual property | This information asset has little intrinsic value, but other assets protected by this device could be attacked if it is compromised. |

**RISK ASSESSMENT**

- Assigns a risk rating or score to each Information asset.
- It is useful in gauging the relative risk to each Vulnerable asset.

**Valuation of Information assets**

- Assign weighted scores for the value to the organization of each Information asset. The csla could range from 1 to 100
- 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)**

- Residual risk is the risk that remains to the information asset even after the existing control has been applied.
- Three general categories of controls
  1. Policies
  2. Programs
  3. Technologies

1. Policies
   - General Security Policy:is an executive level document that specifies the organizations approach and attitude towards information security
   - Program Security Policy :is a planning level document that specifies how security is implemented in the organization

- Issue Specific Policy:take care of specific implementations or applications
- Systems Specific Policy:address the particular use of certain systems

2. Programs
    - Education
    - Training
    - Awareness
3. Security Technologies
    - Technical Implementation Policies

**Access Controls**

- Specially addresses admission of a user into a trusted area of the organization.
- Eg: Computer rooms, Power Rooms.
- Combination of policies , Programs, & Technologies

**Types of Access controls**

Mandatory Access Controls (MACs)

- Give users and data owners limited control over access to information resources.

Nondiscretionary Controls

- 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)

- Implemented at discretion or option of the data user

Lattice-based Access Control

- Variation of MAC - 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. You should also have collected some information about the controls that are already in place. The final summarized document is the ranked vulnerability risk worksheet, a sample of which is shown in the following table.

The worksheet or the list should contain the following fields

**Asse**t: Name of the vulnerable asset

**Asset impact**: The weighted factor analysis value of each asset

**Vulnerability**:Name of the uncontrolled vulnerability

**Vulnerability Likelihood**:range from 0.1 to 1.0

**Risk Rating Factor** :asset impact *Likelihood

| 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 |

**Risk Control Strategies**

**Risk Management** :is the process of identifying vulnerabilities in an organization's information systems and taking carefully reasoned steps to assure the confidentiality, integrity and availability of all the components in the organizations information systems

Four basic strategies to control each of the risks that result from these vulnerabilities.

1. Apply safeguards that eliminate the remaining uncontrolled risks for the vulnerability [Avoidance]
2. Transfer the risk to other areas (or) to outside entities[transference]
3. Reduce the impact should the vulnerability be exploited[Mitigation]
4. Understand the consequences and accept the risk without control or mitigation[Acceptance]

**Avoidance**

It is the risk control strategy that attempts to prevent the exploitation of the vulnerability, and is accomplished by means of

a) Countering threats
b) Removing Vulnerabilities in assets
c) Limiting access to assets
d) Adding protective safeguards.

Three common methods of risk avoidance are

1. Application of policy
2. Application of Training & Education
3. Application of Technology

**Transference**

- Transference is the control approach that attempts to shift the risk to other assets, other processes, or other organizations.
- It may be accomplished through rethinking how services are offered, revising deployment models, outsourcing to other organizations, purchasing Insurance, Implementing Service contracts with providers.

Top 10 Information Security mistakes made by individuals.

1. Passwords on Post-it-Notes
2. Leaving unattended computers on.
3. Opening e-mail attachments from strangers.
4. Poor Password etiquette
5. Laptops on the loose (unsecured laptops that are easily stolen)
6. Blabber mouths ( People who talk about passwords)
7. Plug & Play[Technology that enables hardware devices to be installed and configured without the protection provided by people who perform installations]
8. Unreported Security Violations
9. Always behind the times.
10. Not watching for dangers inside the organization

**Mitigation**

- It is the control approach that attempts to reduce the impact caused by the exploitation of vulnerability through planning & preparation.

- Mitigation begins with the early detection that an attack is in progress and the ability of the organization to respond quickly, efficiently and effectively.

- Includes 3 types of plans.

1. Incident response plan (IRP) -Actions to take while incident is in progress
2. Disaster recovery plan (DRP) - Most common mitigation procedure.
3. Business continuity plan (BCP) - Continuation of business activities if catastrophic event occurs.

**Incident Response Plan (IRP)**

This IRP Plan provides answers to questions such as

1. What do I do now?

2. What should the administrator do first?
3. Whom should they contact?
4. What should they document?

**The IRP Supplies answers.**

For example, a system's administrator may notice that someone is copying information from the server without authorization, signaling violation of policy by a potential hacker or an unauthorized employee.

**The IRP** also enables the organization to take coordinated action that is either predefined and specific or ad hoc and reactive.

**Disaster Recovery Plan (DRP)**

- Can include strategies to limit losses before and during the disaster.
- 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 floodwater recede.
- DRP focuses more on preparations completed before and actions taken after the incident, whereas the IRP focuses on intelligence gathering, information analysis, coordinated decision making, and urgent, concrete actions.

**Business Continuity Plan (BCP)**

- 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 operations center.
- The BCP includes 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.
- Many companies offer this service as a contingency against disastrous events such as fires. Floods, earthquakes, and most natural disasters.

**Acceptance**

- It is the choice to do nothing to protect a vulnerability and do accept the outcome of its exploitation.
- This strategy occurs when the organization has:
  - Determined the level of risk.

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

**Selecting a Risk Control Strategy**

-Level of threat and value of asset play major role in selection of strategy

-Rules of thumb on strategy selection can be applied:

- When vulnerability (flaw or weakness) exists: Implement security controls to reduce the likelihood of a vulnerability being exercised.
- When vulnerability can be exploited: Apply layered protections, architectural designs, and administrative controls to minimize the risk.
- When the attacker's cost is less than his potential gain: Apply protections to increase the attacker's cost.
- When potential loss is substantial: Apply design principles, architectural designs, and technical and non-technical protections to limit the extent of the attack, thereby reducing

the potential for loss.

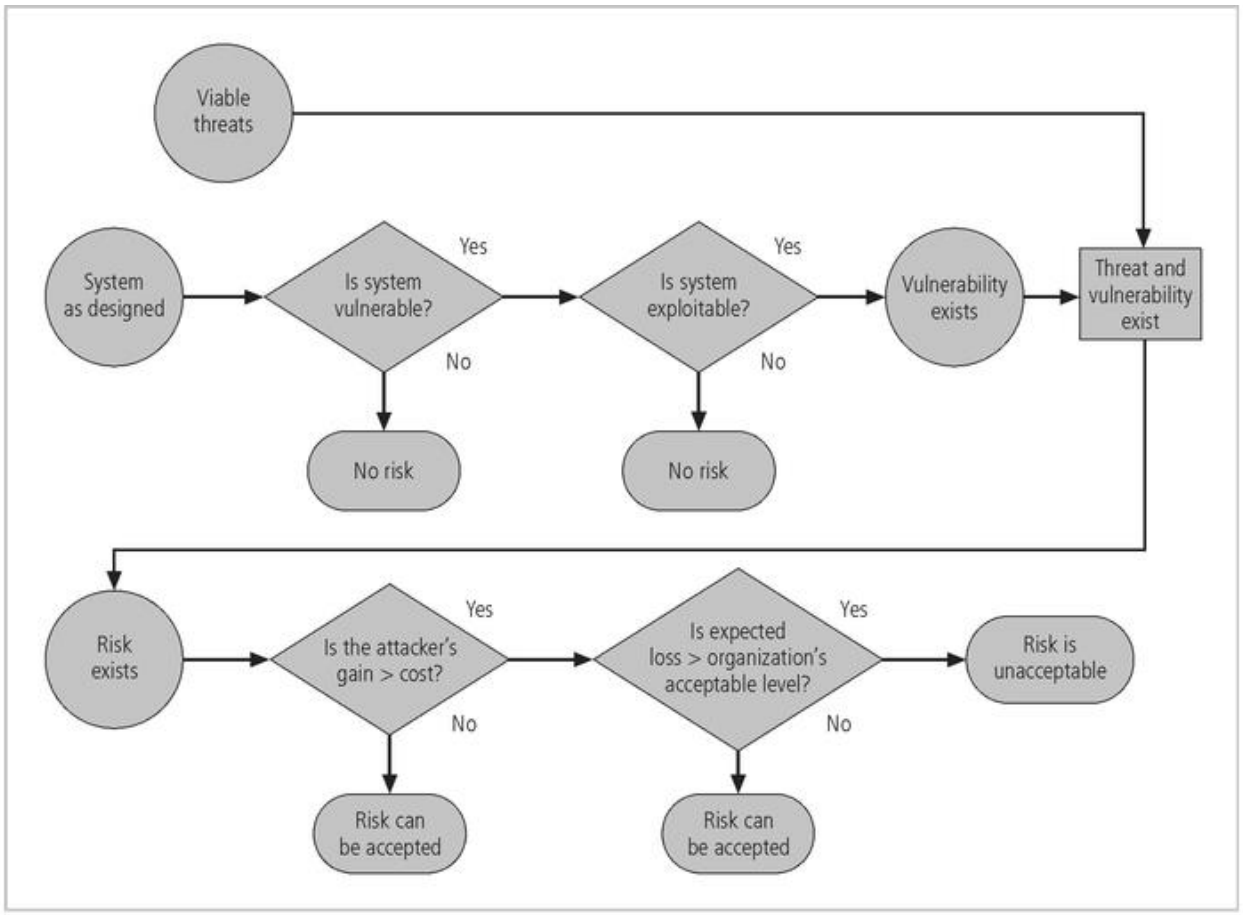
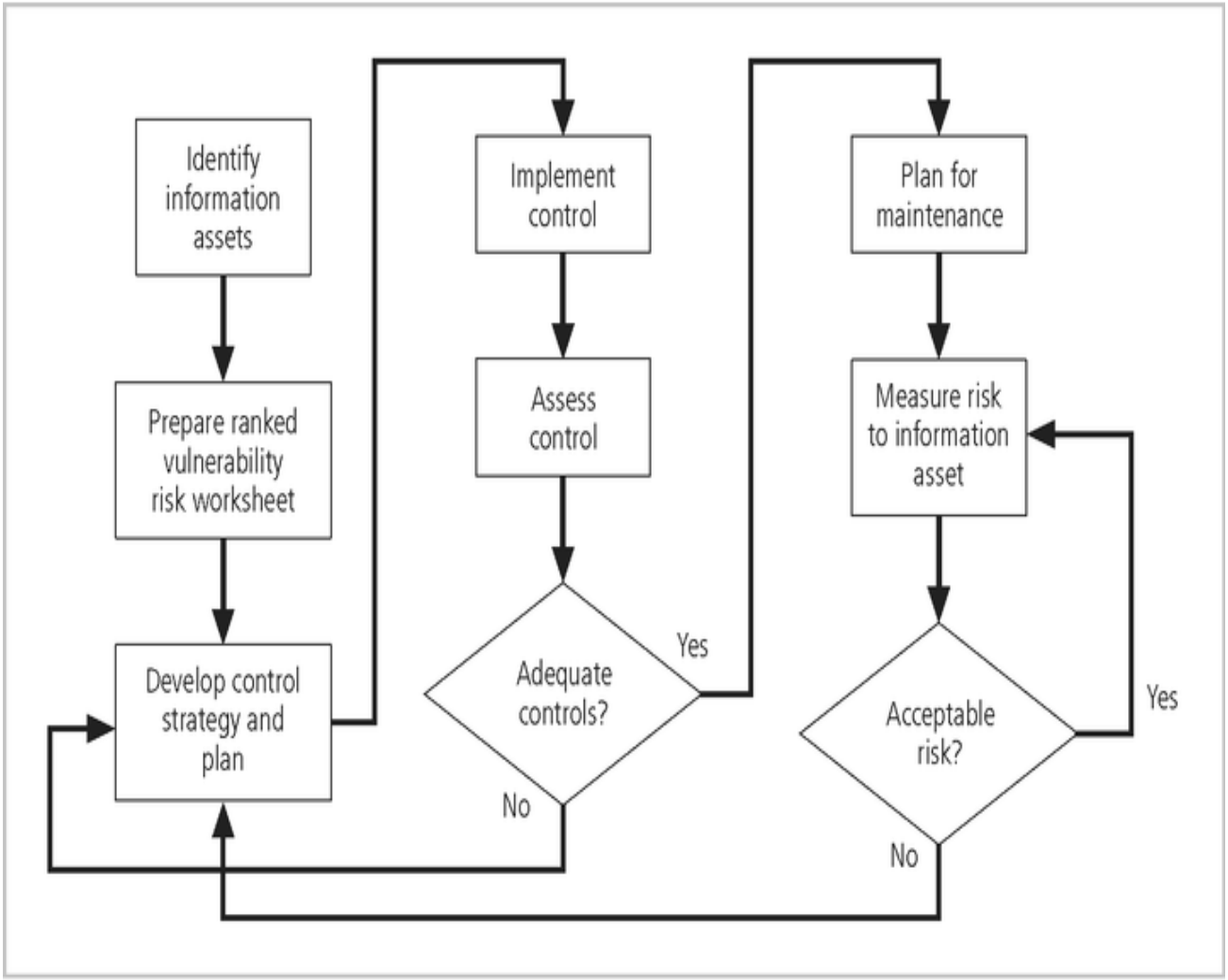



**FIGURE 5-2** Risk Handling Decision Points[7]

**Evaluation, Assessment & Maintenance of Risk Controls**

- Once a control strategy has been implemented, it should be monitored, & measured on an ongoing basis to determine the effectiveness of the security controls and the accuracy of the estimate of the Residual risk
- There is no exit from this cycle; it is a process that continues for as long as the organization continues to function.

# Risk Control Cycle




**Categories of Controls**

- Controlling risk through avoidance, Mitigation or Transference may be accomplished by implementing controls or safeguards.
- Four ways to categorize controls have been identified.

  - **Control function**
    - Preventive or detective
  - **Architectural layer**
    - One or more layers of technical architecture

- **Strategy layer**
    - Avoidance, mitigation …
- **Information security principle**

**Control Function**

- Safeguards designed to defend systems are either preventive or detective.
- Preventive controls stop attempts to exploit a vulnerability by implementing a security principle, such as authentication, or Confidentiality.
- **Preventive controls** use a technical procedure, such as encryption, or some combination of technical means and enforcement methods.
- **Detective controls** – warn organizations of violations of security principles, organizational policies, or attempts to exploit vulnerabilities.
- Detective controls use techniques such as audit trails, intrusion detection and configuration monitoring.

**Architectural Layer**

- Controls apply to one or more layers of an organization's technical architecture.
- The following entities are commonly regarded as distinct layers in an organization's Information architecture.

1. Organizational policy.
2. External Networks.
3. Extranets ( or demilitarized zones )
4. Intranets ( WANs and LANs )
5. Network devices that interface network zones.(Switches, Routers, firewalls and hubs)
6. Systems [ Mainframe, Server, desktop]
7. Applications.

**Strategy Layer**

Controls are sometimes classified by the risk control strategy they operate within:

1. Avoidance
2. Mitigation
3. transference

**Information security Principles**

Characteristics of Secure Information

1. Confidentiality
2. Integrity
3. Availability
4. Authentication
5. Authorization
6. Accountability
7. Privacy

**Confidentiality**: The control assures the confidentiality of data when it is stored, processed, or transmitted. An example of this type of control is the use of Secure Sockets Layer (SSL) encryption technology to secure Web content as it moves from Web server to browser.

**Integrity**: The control assures that the information asset properly, completely, and correctly receives, processes, stores, and retrieves data in a consistent and correct manner .Ex: Use of parity or cyclical redundancy checks in data transmission protocols.

**Availability**: The control assures ongoing access to critical information assets. Ex: Deployment of a network operations center using a sophisticated network monitoring toolset.

**Authentication**: The control assures that the entity (person or computer) accessing information assets is in fact the stated entity. Ex: The use of cryptographic certificates to establish SSL connections, or the use of cryptographic hardware tokens such as SecurID cards as a second authentication of identity.

**Authorization**: The control assures that a user has been specifically and explicitly authorized to access, update, or delete the contents of an information asset. Ex: Use of access control lists and authorization groups in the Windows networking environment. Another example is the use of a database authorization scheme to verify the designated users for each function.

**Accountability**: The control assures that every activity undertaken can be attributed to a specific named person or automated process. Ex: Use of audit logs to track when each user logged in and logged out of each computer.

Privacy: The control assures that the procedures to access, update, or remove personally identifiable information comply with the applicable laws and policies for that kind of information.

**Feasibility Studies**

- Before deciding on the strategy (Avoidance, transference, mitigation, or acceptance), for a specific vulnerability, all the economic and non-economic consequences of the vulnerability facing the information asset must be explored.
- **Cost Avoidance**- It is the process of avoiding the financial impact of an incident by implementing a control.
- Includes
    1. Cost Benefit analysis
    2. Organizational feasibility
    3. Operational Feasibility
    4. Technical Feasibility
    5. Political feasibility.

**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 Cost Benefit Analysis (CBA)**

- The most common approach for a project of information Security controls and safeguards is the economic feasibility of implementation.
- Begins by evaluating the worth of information assets are compromised.
- It is only common sense that an organization should not spend more to protect an asset than it is worth.
- The formal process to document this is called a cost benefit analysis or an economic feasibility study.

**CBA: Cost Factors**

- Some of the items that the cost of a control or safeguard include:
- Cost of Development or Acquisition
- Training Fees
- Cost of implementation.

- Service Costs
- Cost of Maintenance

**CBA: Benefits**

- Benefit is the value that the organization recognizes by using controls to prevent losses associated with a specific vulnerability.
- This is usually determined by valuing the information asset or assets exposed by the vulnerability and then determining how much of that value is at risk.

**CBA: Asset Valuation**

- Asset Valuation is the process of assigning financial value or worth to each information asset.
- The valuation of assets involves estimation of real and perceived costs associated with the design, development, installation, maintenance, protection, recovery, and defense against market loss and litigation.
- These estimates are calculated for each set of information bearing systems or information assets.
- There are many components to asset valuation.

**CBA: Loss Estimates**

- Once the worth of various assets is estimated examine the potential loss that could occur from the exploitation of vulnerability or a threat occurrence.
- This process results in the estimate of potential loss per risk.
- The questions that must be asked here include:
    - What damage could occur, and what financial impact would it have?
    - What would it cost to recover from the attack, in addition to the costs above?
    - What is the single loss expectancy for each risk?

**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?

**Loss estimates**

**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
- 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**
- 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
- Failure to support a standard of due care or due diligence can open an organization to legal liability

**Best Business Practices**

- Security efforts that provide a superior level of protection of information are referred to as best business practices
- 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 in application of benchmarking and best practices**

- 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.
- One last issue to consider is that simply knowing what was going on a few years ago, as in benchmarking, doesn't necessarily tell us what.

**Baselining**

- Baselining is the analysis of measures against established standards,
- In information security, baselining is comparing security activities and events against the organization's future performance.
- When baselining it is useful to have a guide to the overall process

**Feasibility Studies**

This indicates how well the organization is prepared to undertake the control measures

**Organizational Feasibility**

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

- Addresses user acceptance and support, management acceptance and support, and the overall requirements of the organization's stake holders.

- Sometimes known as behavioral feasibility, because it measures the behavior of users.
- One of the fundamental principles of systems development is obtaining user buy in on a project and one of the most common methods for obtaining user acceptance and support is through user involvement obtained through three simple steps:

- Communicate
- Educate
- Involve

**Technical Feasibility**

- The project team must also consider the technical feasibilities associated with the design, implementation, and management of controls.
- Examines whether or not the organization has or can acquire the technology necessary to implement and support the control alternatives.

**Political feasibility**

- For some organizations, the most significant feasibility evaluated may be political
- Within Organizations, political feasibility defines what can and cannot occur based on the consensus and relationships between the communities of interest.
- The limits placed on an organization's actions or a behavior by the information security controls must fit within the realm of the possible before they can be effectively implemented, and that realm includes the availability of staff resources.

**Risk Management Discussion Points**

Not every organization has the collective will to manage each vulnerability through the application of controls

- Depending on the willingness to assume risk, each organization must define its risk appetite
- Risk appetite defines the quantity and nature of risk that organizations are willing to accept as they evaluate the tradeoffs between perfect security and unlimited accessibility

**Residual Risk**

- When we have controlled any given vulnerability as much as we can, there is often risk that has not been completely removed or has not been completely shifted or planned for this remainder is called residual risk.
- To express it another way, "Residual risk is a combined function of
    1. A threat less the effect of some threat –reducing safeguards.

2. Vulnerability less the effect of some vulnerability- reducing safeguards.
3. an asset less the effect of some asset value-reducing safeguards “

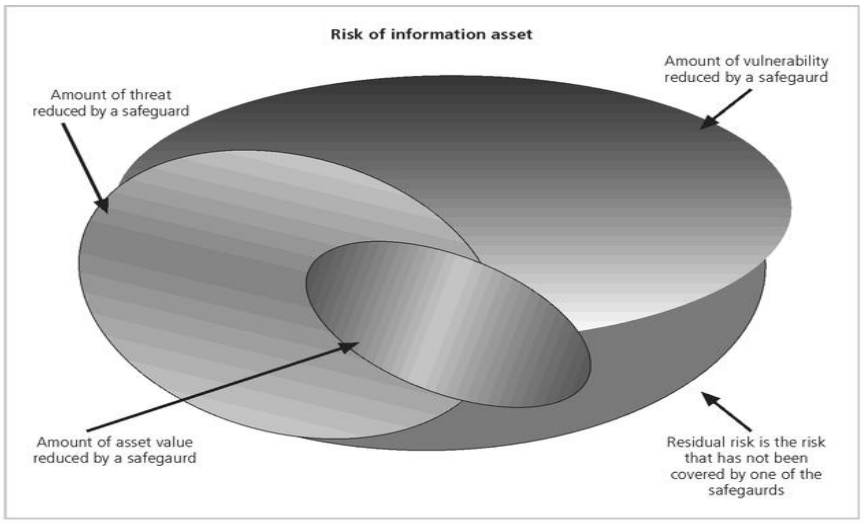



**FIGURE 5-4** Risk Residual

**Documenting Results**

- At minimum, each information asset-vulnerability pair should have a documented control strategy that clearly identifies any residual risk remaining after the proposed strategy has been executed.
- Some organizations document the outcome of the control strategy for each information asset-vulnerability pair as an action plan
- This action plan includes concrete tasks, each with accountability assigned to an organizational unit or to an individual

**Recommended Practices in Controlling Risk**

- We must convince budget authorities to spend up to the value of the asset to protect a particular asset from an identified threat
- Each and every control or safeguard implemented will impact more than one threat-asset pair

**Qualitative Measures**

- The spectrum of steps described above was performed with real numbers or best guess estimates of real numbers-this is known as a quantitative assessment.

- However, an organization could determine that it couldn't put specific numbers on these values.
- Fortunately, it is possible to repeat these steps using estimates based on a qualitative assessment.
- Instead of using specific numbers, ranges or levels of values can be developed simplifying the process

**Delphi Technique**

- One technique for accurately estimating scales and values is the Delphi Technique.
- The Delphi Technique, named for the Oracle at Delphi, is a process whereby a group of individuals rate or rank a set of information
- The individual responses are compiled and then returned to the individuals for another iteration
- This process continues until the group is satisfied with the result.

1. Describe risk transference. Describe how outsourcing can be used for risk transference.
2. Describe risk mitigation. What three planning approaches are discussed in the text as opportunities, to mitigate risk?
3. List any four Information Security Policies.
4. How do you categories the components of an information system? Explain.

What do you mean by access control? Describe the different types of access control and risk control strategies

## LOGICAL DESIGN

### 1.INFORMATION SECURITY POLICY, STANDARDS AND PRACTICES -

- Creation of information security program begins with creation and/or review of organization's information security policies, standards, and practices
- Then, selection or creation of information security architecture and the development and use of a detailed information security blueprint creates plan for future success
- Security education and training to successfully implement policies and ensure secure environment

**Why Policy?**

- A quality information security program begins and ends with policy
- Policies are least expensive means of control and often the most difficult to implement
- Some basic rules must be followed when shaping a policy:
    - Never conflict with law
    - Stand up in court
    - Properly supported and administered
    - Contribute to the success of the organization
    - Involve end users of information systems

**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
- **Standards**: more detailed statements of what must be done to comply with policy
- **de-facto standards** are informally accepted standards
- **de jure standards**-are published formal standards
- **Practices, procedures and guidelines** effectively explain how to comply with policy
- The **mission** of an organization is the written statement of organization's purpose
- The **vision** of an organization is the written statement of organization's goal
- the **strategic planning** is the process of conducting an organization towards its vision through accomplishing its mission
- The **security policy** is set of rules for the protection of organization's assets
- An **Information security policy** gives the rules for protection of information assets of an organization.
- For a policy to be effective it must be
    - Properly disseminated
    - Read
    - Understood
    - Agreed to by all members of organization

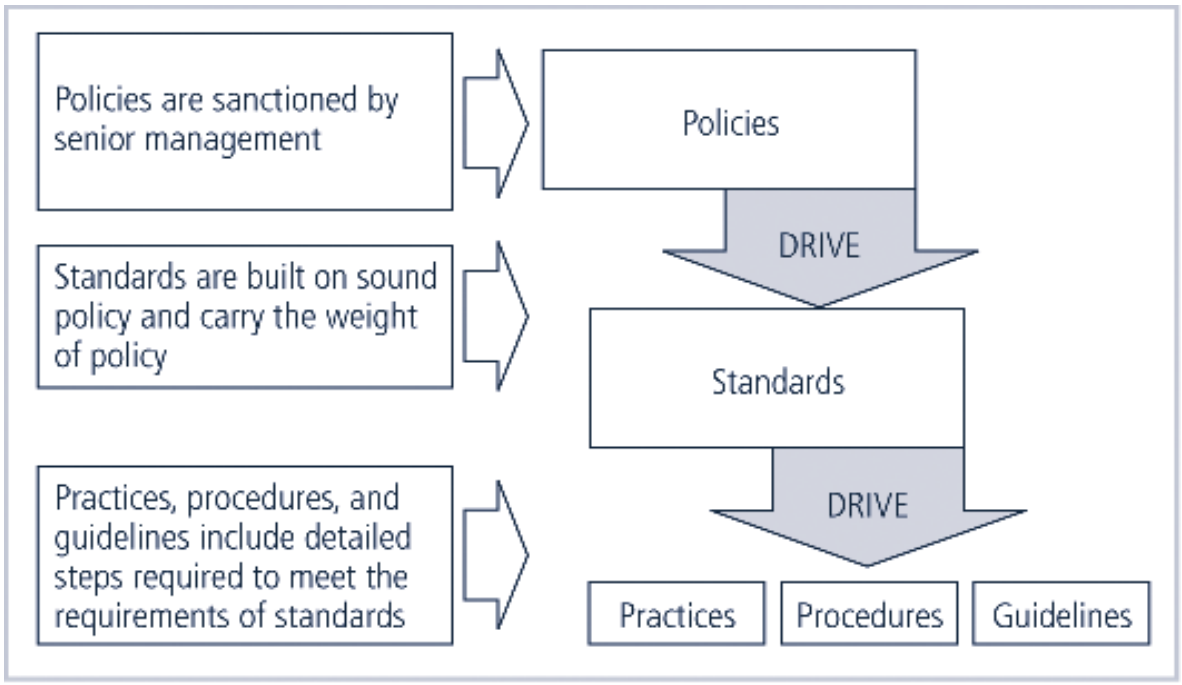



**FIGURE 5-1** Policies, Standards, and Practices

**Types of Policies**

- Enterprise information Security program Policy(EISP)
- Issue-specific information Security Policy ( ISSP)
- Systems-specific information Security Policy (SysSP)

**Enterprise Information Security Policy (EISP)**

- Also Known as a general Security policy, IT security policy, or information security policy.
- This supports mission, vision and strategic goals of an organization.
- Sets strategic direction, scope, and tone for all security efforts within the organization
- This is an **Executive level document** usually drafted by or with CIO of the organization ,which do not undergo continuous modification
- Assigns responsibilities to various areas of information security
- EISP Guides development, implementation, and management of information security program

**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

The following are some of the terms of ISSP statement :

- 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

**Systems-Specific Policy (SysSP)**

- SysSPs are frequently codified as standards and procedures to be used when configuring or maintaining systems
- They are formally written documents and are distributed to users
- Systems-specific policies fall into two groups:
- **Access control lists (ACLs)** consist of the access control lists, matrices, and capability tables governing the rights and privileges of a particular user to a particular system
- **Configuration rules** comprise the specific configuration codes entered into security systems to guide the execution of the system

**ACL Policies**

ACLs allow a configuration to restrict access from anyone and anywhere.

- They may be lists, matrics and capabilities table containing the rights and privileges of a specific user to a specific system.
- An ACL specifies which users or system processes are granted access to objects ,as well what operations are allowed on given objects.
- The most common privileges include the ability to read a file to write to the file or files, and to execute the file.
- 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

**Capability table**, is very similar to ACL and it contains details about which subjects and objects a user or group can access

**Configuration rules**

-They contain configuration codes entered into the security systems to guide the execution of the system, when information is handled by that system

**Policy management**

Policies are document that must be managed as they constantly change.

**security policies** must have:

- Individual responsible for the policy (policy administrator)
- A schedule of reviews
- Procedures and practices in the review
- Specific policy issuance and revision date
- Automated policy management

**THE INFORMATION SECURITY BLUEPRINT**

- It is the basis for the design, selection, and implementation of all security policies, ongoing policy management, risk management programs  education and training programs, and technological controls, and maintenance of the security program
- More detailed version of **security framework**, which is an outline of overall information security strategy for organization and a road map for planned changes to the information security environment of the organization.
- Should specify tasks to be accomplished and the order in which they are to be realized.
- Should also serve as a scalable, upgradeable, and comprehensive plan for the information security needs for coming years.

**2. SECURITY MODELS**

**2.1 ISO 17799/BS 7799 series**

- One of the most widely referenced and often discussed security models is the Information Technology – Code of Practice for Information Security Management, which was originally published as British Standard BS 7799
- In 2000, this Code of Practice was adopted as an international standard framework for information security by the International Organization for Standardization (ISO
- It can be used by any organization that needs to establish a comprehensive information security management program or to improve its current information security practices.

**Objectives of ISO 17799**

Organizational Security Policy is needed to provide management direction and support.

**Ten Sections of ISO/IEC 17799**

a. **Organizational Security Policy**:-Provide guidelines and management advice for improving information security.
b. **Organizational Security Infrastructure**:-Facilitate information security management within the organization
c. **Asset Classification and Control** :-Carry out an inventory of assets and protect these assets effectively.
d. **Personnel Security:-**Minimize the risks of human error, theft, fraud or the abuse of equipment
e. **Physical and Environmental Security** :-Prevent the violation ,disruption of industrial facilities and data.
f. Communications and Operations Management :-Ensure adequate and reliable operations of information processing devices.
g. **System Access Control** :-Control access to information
h. **System Development and Maintenance**:Ensure that security is incorporated into information systems
i. **Business Continuity Planning**
j. **Compliance**

- This is concise process for evaluating ,implementing, maintaining and managing information security
- The overall methodology for information security management system(ISMS) is given below:

**Plan**

- Define the ISMS scope and the organizations security practices.
- Identify and assess risks
- Select control objectives and controls that will help manage these risks
- Prepare the statement of applicability

**Do**

- Formulate and implement a risk mitigation plan.
- Implement the previously selected controls in order to meet the control objectives

**Check**

- Perform monitoring procedures
- Conduct periodic reviews to verify the effectiveness of the ISMS
- Review the levels of acceptable and residual risk.
- Periodically conduct internal ISMS audits

**Act**

- Implement identified ISMS improvements.
- Take appropriate corrective and preventive action
- Maintain communications with all stakeholders
- Validate improvements.

**Alternate Security Models available other than ISO 17799/BS 7799**

## 2.2 NIST SECURITY MODELS

- 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.
- 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 (csrc.nist.gov).

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**

- Generally accepted Principles and practices for Security Information Technology Systems.
- 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
    - Security is an Integral Element of Sound Management
    - Security Should Be Cost-Effective
    - Systems Owners Have Security Responsibilities Outside Their Own Organizations
    - Security Responsibilities and Accountability Should Be Made Explicit
    - Security Requires a Comprehensive and Integrated Approach
    - Security Should Be Periodically Reassessed
    - Security is Constrained by Societal Factors
    - 33 Principles enumerated

**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.
- The table of contents for Publication 800-18 is presented in the following.

**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**

1. Personnel Security
2. Physical Security
3. Production, Input/Output Controls
4. Contingency Planning
5. Hardware and Systems Software
6. Data Integrity

7. Documentation
8. Security Awareness, Training, and Education
9. Incident Response Capability

**Technical Controls**

- Identification and Authentication
- Logical Access Controls
- Audit Trails

**NIST SP 800-26**: *Security Self-Assessment Guide for IT systems*

**NIST SP 800-26 Table of contents**

**Management Controls**

1. Risk Management
2. Review of Security Controls
3. Life Cycle Maintenance
4. Authorization of Processing (Certification and Accreditation)
5. System Security Plan

**Operational Controls**

6. Personnel Security
7. Physical Security
8. Production, Input/Output Controls
9. Contingency Planning
10. Hardware and Systems Software
11. Data Integrity
12. Documentation
13. Security Awareness, Training, and Education
14. Incident Response Capability

**Technical Controls**

15. Identification and Authentication
16. Logical Access Controls
17. Audit Trails

**IETF Security architecture**

The Internet Engineering Task force has given the following points for good functioning of security systems

RFC 2196 –Site security handbook ,provides a good functional discussion of important security issues.

RFC 2196 covers five basis areas of security with detailed discussions on development and implementation.

This has the following five sections:

1. Introduction
    - 1.1 Purpose of this work
    - 1.2 Audience
    - 1.3 Definitions
    - 1.4 Related Work
    - 1.5 Basic approach
    - 1.6 Risk Assessment
2. Security policies
    - 2.1 What is security policy and why have one ?
    - 2.2 What makes a good security policy ?
    - 2.3 Keeping the policy Flexible
3. Architecture
    - 3.1 Objectives
    - 3.2 Network and service configuration
    - 3.3 Firewalls
4. Security services and Procedures
    - 4.1 authentication
    - 4.2 Confidentiality
    - 4.3 Integrity
    - 4.4 Authorization
    - 4.5 Access
    - 4.6 Auditing
    - 4.7 securing backups

5. Security incident handling
    5.1 Preparing and planning for incident handling
    5.2 Notifications and points of contact
    5.3 Identifying an incident
    5.4 Handling of an Incident
    5.5 Aftermath of an Incident
    5.6 responsibilities
6. Ongoing Activities
7. Tools and Locations
8. Mailing lists and other resources
9. References

## 2.3 VISA INTERNATIONAL SECURITY MODEL

- It 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:** it contains 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.

**Baselining & Best Business Practices**

- Baselining 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 baselining 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.
- Of 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.

## 3. DESIGN OF SECURITY ARCHITECTURE

**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.

**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
    - policies
    - people (education, training, and awareness programs)
    - technology

**Levels of controls**

- **Management controls** address 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** deal 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** 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.

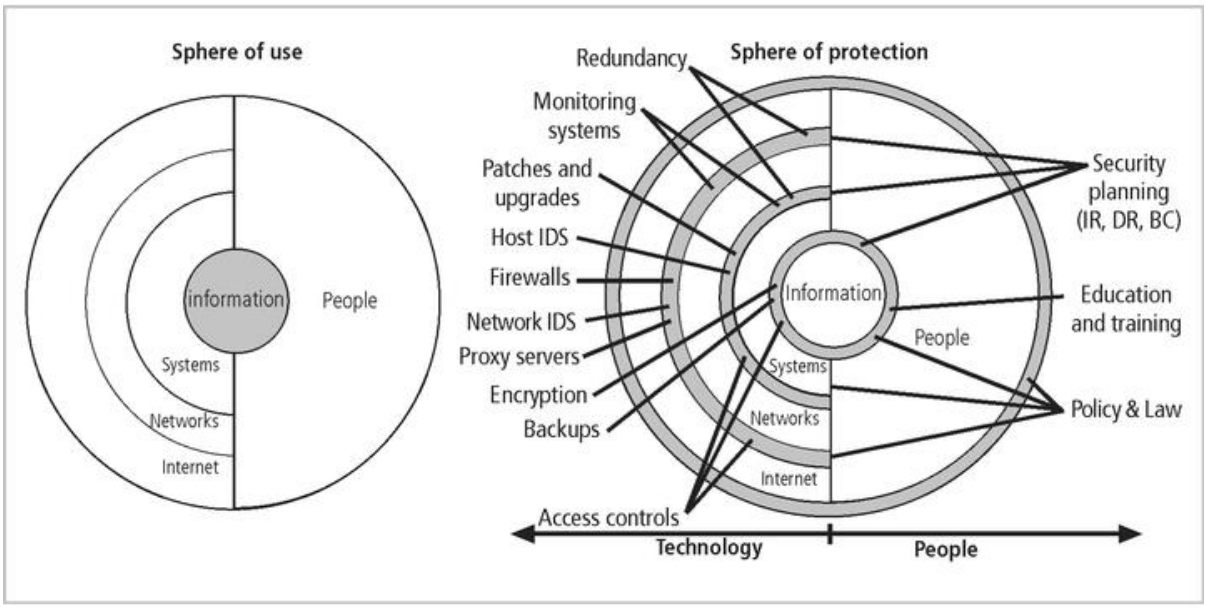



**FIGURE 6-16** Spheres of Security

- As illustrated in the sphere of protection, a variety of controls can be used to protect the information.
- The items of control shown in the figure are not intended to be comprehensive but rather illustrate individual safeguards that can protect the various systems that are located closer to the center of the sphere.
- However, because people can directly access each ring as well as the information at the core of the model, the side of the sphere of protection that attempt to control access by

relying on people requires a different approach to security than the side that uses technology.

**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.

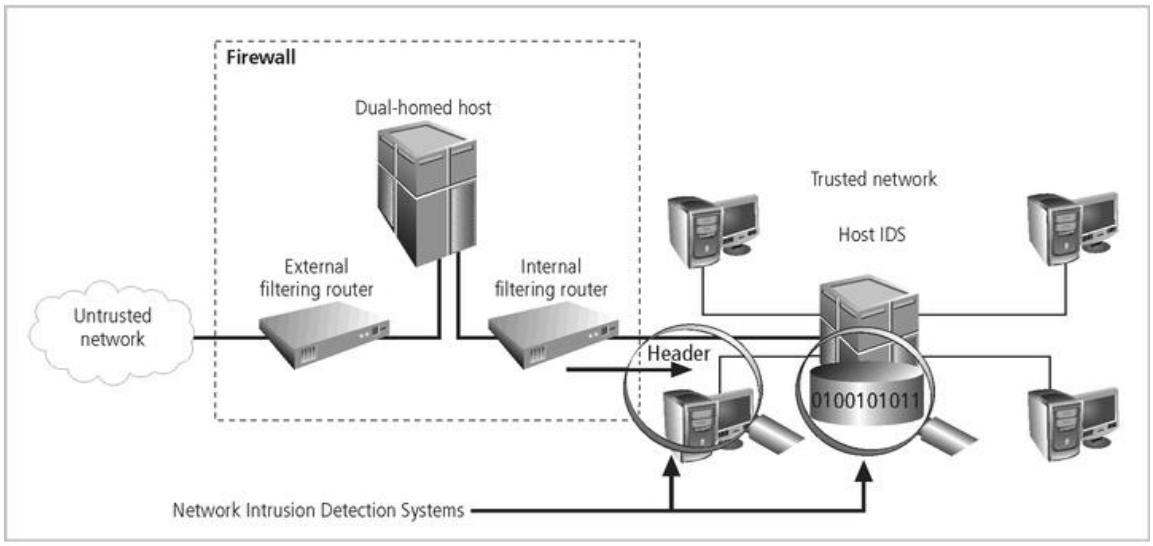



**FIGURE 6-18** Defense in Depth

**Security Perimeter**

- A Security Perimeter is the first level of security that protects all internal systems from outside threats.
- Unfortunately, the perimeter does not protect against internal attacks from employee threats, or on-site physical threats.
  - Security perimeters can effectively be implemented as multiple technologies that segregate the protected information from those who would attack it.
  - Within security perimeters the organization can establish security domains, or areas of trust within which users can freely communicate.
  - The presence and nature of the security perimeter is an essential element of the overall security framework, and the details of implementing the perimeter make up a great deal of the particulars of the completed security blueprint.
  - The key components used for planning the perimeter are presented in the following sections on firewalls, DMZs, proxy servers, and intrusion detection systems.

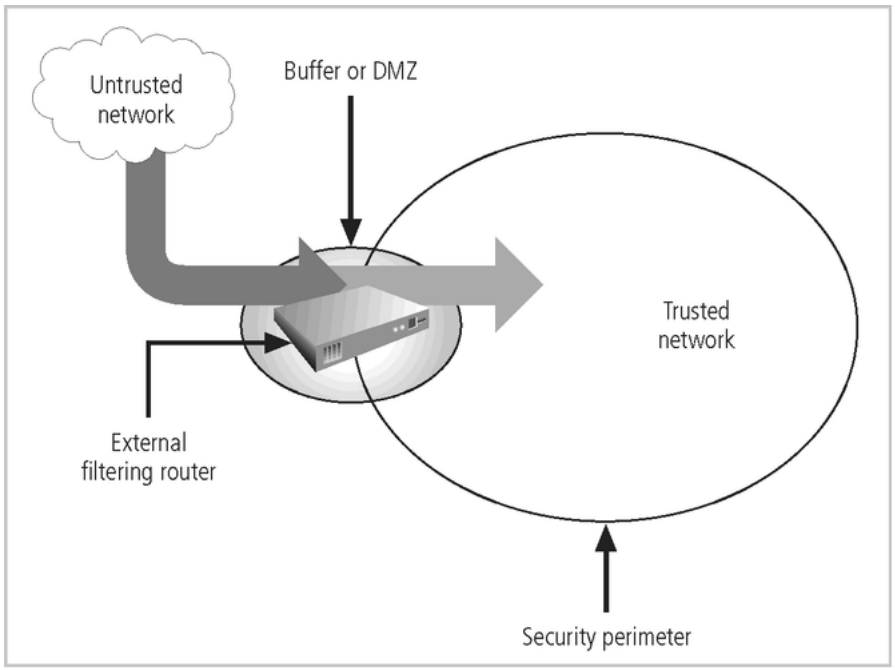



**FIGURE 6-19** Security Perimeters and Domains

**Key Technology Components**

- Other key technology components

**Firewalls:**

- A **firewall** is a device that selectively discriminates against information flowing into or out of the organization.
- firewalls are frequently used to prevent unauthorized internet users from accessing private networks connected to the internet, especially
  intranets.
- All messages entering or leaving the intranet pass through the firewall ,which examines each message and blocks those that do not meet the specified security criteria.
- Firewalls are usually placed on the security perimeter, just behind or as part of a **gateway router**.
- The gateway router connects the organizations system with the outside world
- 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.
- firewalls are frequently used to prevent unauthorized internet users from accessing private networks connected to the internet, especially
  intranets.
- The types of firewalls includes: Network-level firewalls, Circuit Level Firewalls, Application level Firewalls, stateful Multilevel firewalls

**DMZ**

- The **DMZ** (demilitarized zone) is a computer host or small network inserted as a neutral zone between a company's private network and the outside public network
- It prevents outside users from getting direct access to a server that has company data
- 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.
- The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN) an external attacker only has access to equipment in the DMZ, rather than any other part of the network.

**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**.

- When an outside client requests a particular Web page, the proxy server receives the request as if it were the subject of the request, then asks for the same information from the true Web server(acting as a proxy for the requestor), and then responds to the request as a proxy for the true Web server.
- For more frequently accessed Web pages, proxy servers can cache or temporarily store the page, and thus are sometimes called **cache servers.**
- They intercept all messages entering and leaving the network
- The proxy server effectively hides the true network addresses.
- They perform action on behalf of another system in the network.

- The outside client will not know whether the requested web page is from proxy system or the original system.
- They give access to the requested web page but do not allow them to directly gain access to the internal network.
- The more frequently accessed pages are stored temporarily in cache servers.

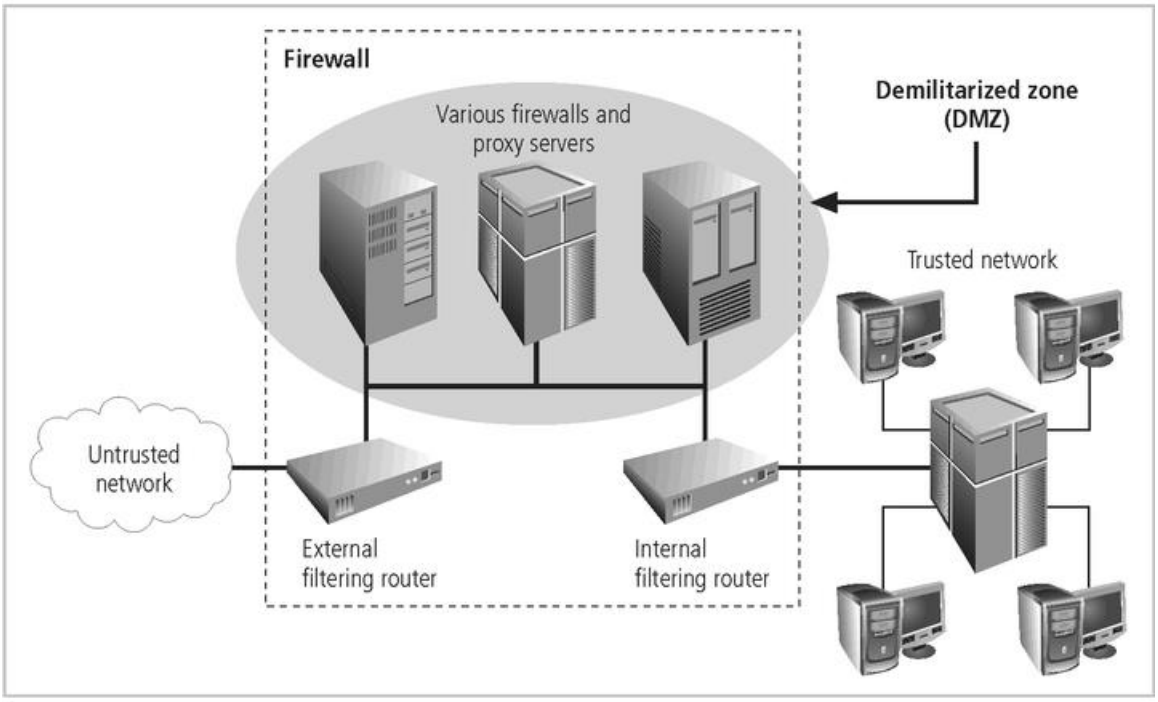



**FIGURE 6-20** Firewalls, Proxy Servers, and DMZs

**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**.
- They detect unauthorized activity within inner network, or on individual machines, organization.
- Many IDSs enable administrators to configure systems to notify them directly of trouble via email or pages.
- **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.
- Host based IDS resides on a particular computer or server and monitors activity only on that system.
- They learn the configuration of systems and assign priorities to files depending on its value and alert the administrator when any suspicious activity is performed.

**Advantages of HIDS:**

- This can detect local events on host systems and detect attacks
- The functions on host systems, where encrypted traffic will have been decrypted and is available for processing.
- They are not affected by use of switched network protocols.
- They can detect inconsistencies in how applications and systems programs were used by examining records stored in audit logs.

**Disadvantages of HIDS:**

- They pose more management issues
- It is vulnerable both to direct attacks and attacks against host operating system.
- It does not detect multi host scanning or scanning of non-host network devices.
- They are susceptible to some denial of service attacks

**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).
- To detect attack ,NIDS look for attack patterns.
- This is implemented by using special implementation of TCP/IP stack.
- NIDs looks for invalid data packets.
- Both host-and network based IDSs require a database of previous activity.

**Advantages of NIDS**

- Good network design and placement of NIDS can enable organization to use a few devices to monitor large network**.**
- NIDs are usually passive and can be deployed into existing networks with little disruption to normal network operations.
- NIDs not usually susceptible to direct attck and may not be detectable by attackers.

**Disadvantages of NIDs:**

- They can become overwhelmed by network volume and fail to recognize attacks.
- They require access to all traffic to be monitored.
- It cannot analyze encrypted packets.
- They cannot reliably ascertain if attack was successful or not
- Some forms of attack are nor easily discerned by NIDs, specifically those involving fragmented packets.

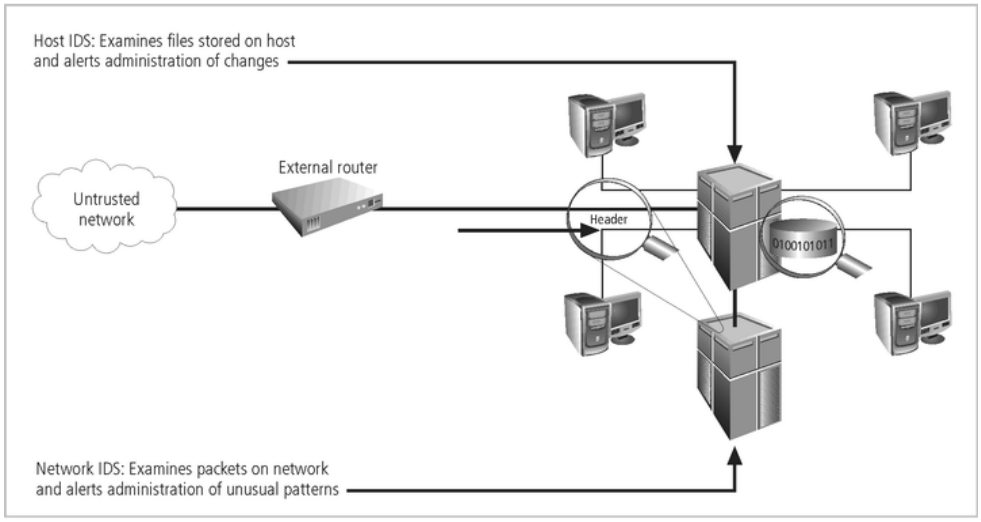



**FIGURE 6-21** Intrusion Detection Systems

## Security Education, Training, and Awareness Program

- As soon as general security policy exists, policies to implement **security education, training and awareness (SETA)** program should follow.
- SETA is a control measure designed to reduce accidental security breaches by employees.

- Security education and training builds on the general knowledge the employees must possess to do their jobs, familiarizing them with the way to do their jobs securely
- The SETA program consists of three elements: security education; security training; and security awareness
- The purpose of SETA is to enhance security by:
    - Improving awareness of the need to protect system resources.
    - Developing skills and knowledge so computer users can perform their jobs more securely.
    - Building in-depth knowledge, as needed, to design, implement, or operate security programs for organizations and systems.

**Security Education**

- Everyone in an organization needs to be trained and aware of information security, but not every member of the organization needs a formal degree or certificate in information security.
- A number of universities have formal coursework in information security.
- For those interested in researching formal information security programs, there are resources available, such as the NSA-identified Centers of Excellence in Information Assurance Education.

**Security Training**

- It involves providing members of the organization with detailed information and hands-on instruction to prepare them to perform their duties securely.
- Management of information security can develop customized in-house training or outsource the training program.

**Security Awareness**

- One of the least frequently implemented, but most beneficial programs is the security awareness program
- Designed to keep information security at the forefront of users' minds

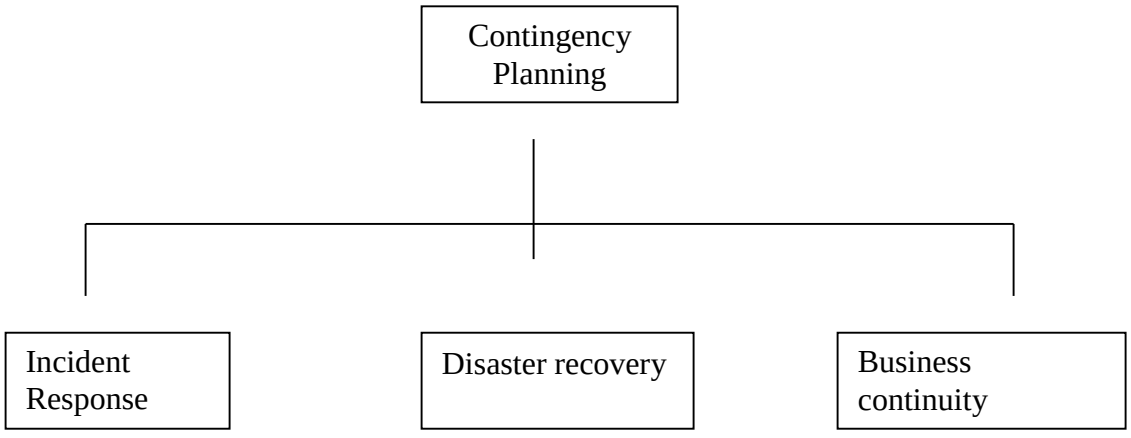
- Need not be complicated or expensive
- If the program is not actively implemented, employees may begin to "tune out" and risk of employee accidents and failures increases

## 4. PLANNING FOR CONTINUITY

### Contingency Planning (CP)

- 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.
- 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. and Testing and revising the strategy.

**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

**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.

**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, Probable, and 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

**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.

**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.

**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.

**Business Continuity Plan (BCP)**

- 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.

**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. It is the pinnacle of contingency planning, a duplicate facility that needs only the latest data backups and the personnel to function as a fully operational twin of the original. Disadvantages include the need to provide maintenance for all the systems and equipment in the hot site, as well as physical and information security.

**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, the negotiations

for arranging the time-share, and associated arrangements, should one or more parties decide to cancel the agreement or to sublease its options.

**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.

## PHYSICAL DESIGN

### 1.SECURITY TECHNOLOGY

**Physical design of the SecSDLC:**

The physical design of secSDLC consists of two major parts:

- Security Technology
- Physical security

Physical design uses logical design as its blueprint

The following will be the end results of physical design:

- Selected technologies to implement information security
- A successful solution
- Physical security measures
- Full equipped organization to create project plans in the implementation phase.

**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.
- A firewall can be either be software based and hardware based and is used to help to maintain secure network.

- Its primary objective is to control the incoming and outgoing network traffic by analysing the data packets and determining whether it should be allowed through or not based on the predetermined rule set.
- A network firewall builds a bridge between an internal network that is assumed to be secure and trusted network, and another networks ,usually and external network, such as the internet, that is assumed to be insecure and untrusted network.

- 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

**Firewall Developement**

There are five recognized generations of firewalls.

***First Generation***

- They are Called as packet filtering firewalls
- Examines every incoming packet header and selectively filters packets based on
  - address, packet type, port request, and others 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
- The permissible addresses are maintained through the access control list(ACL) by the firewall administrator.
- In the advanced version,the filtering of data packets could also be done based on services and protocols.
- This generation of firewalls could not detect IP spoofing attacks.

***Second Generation***

- This is 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 in the DMZ
- 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***

- This is called Stateful inspection firewalls
- 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 in the conversation by recording which station sent what packet and when
- 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 pass
- 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***

- Dynamic packet filtering firewalls belongs to 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 does this 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
- It evaluates packets at multiple layers of the protocol stack, by checking security in the kernel as data is passed up and down the stack
- Cisco implemented this firewall known as **Centri firewall** with three components
    - Interceptor/Packet Analyzer
    - Security Verification Engine(SVEN)
    - Kernel Proxies.

**Firewall Architectures**

The approaches to build an effective firewall could combine the usage of more than one type of firewall mechanism.

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

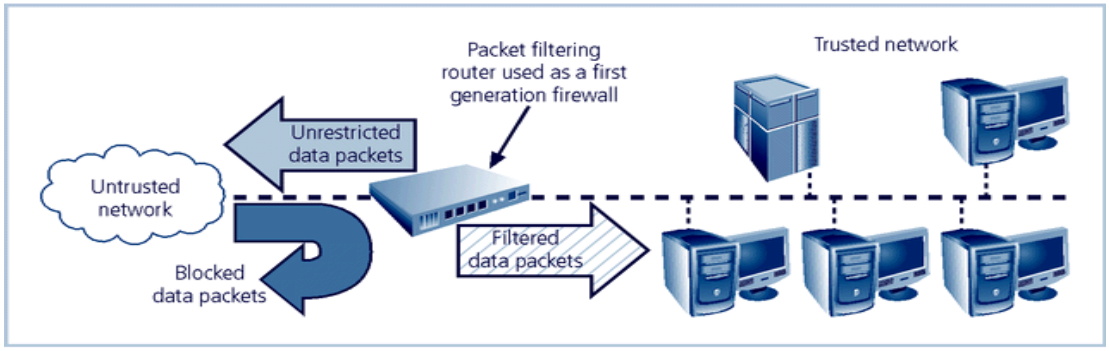



**FIGURE 8-2** Packet Filtering Firewall

***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

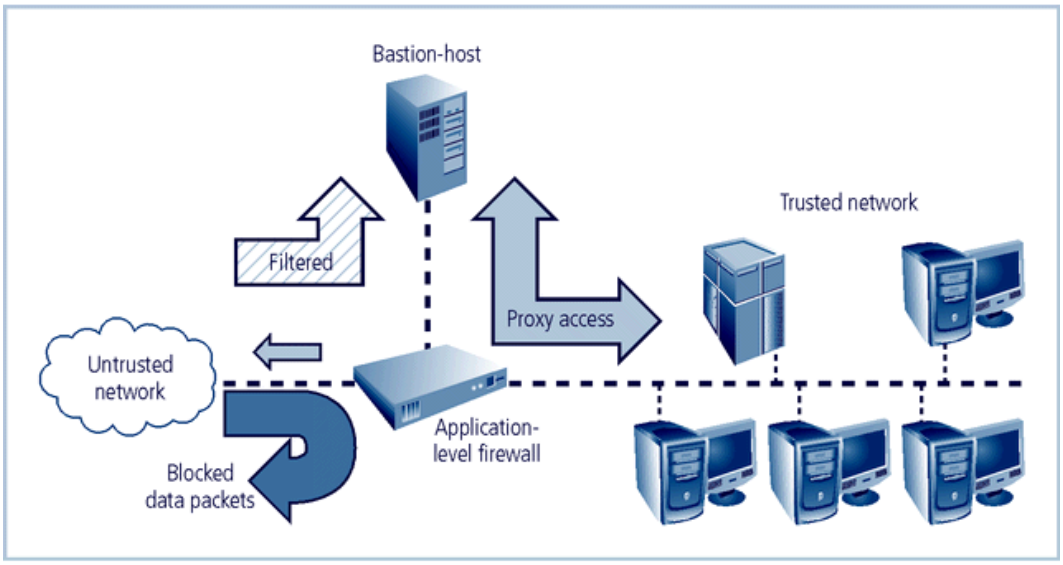



**FIGURE 8-3** Screened Host Firewall

***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

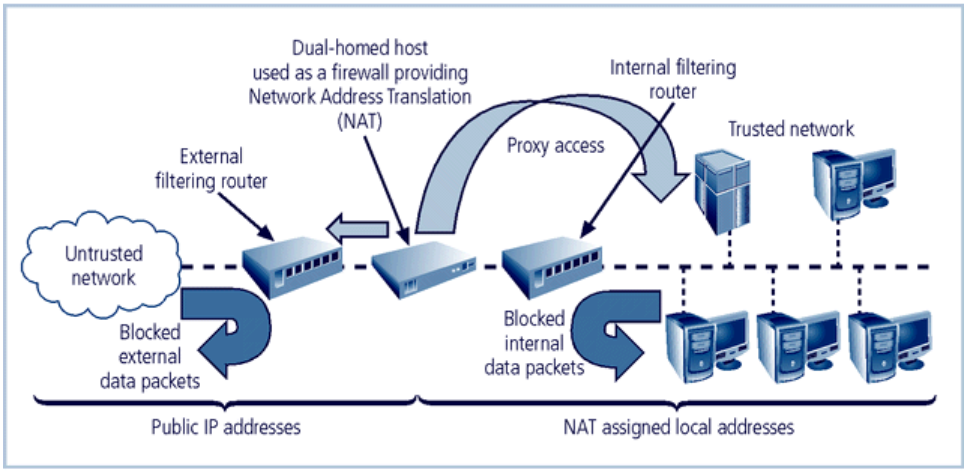



**FIGURE 8-4** Dual-homed Host Firewall

***Screened-Subnet 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

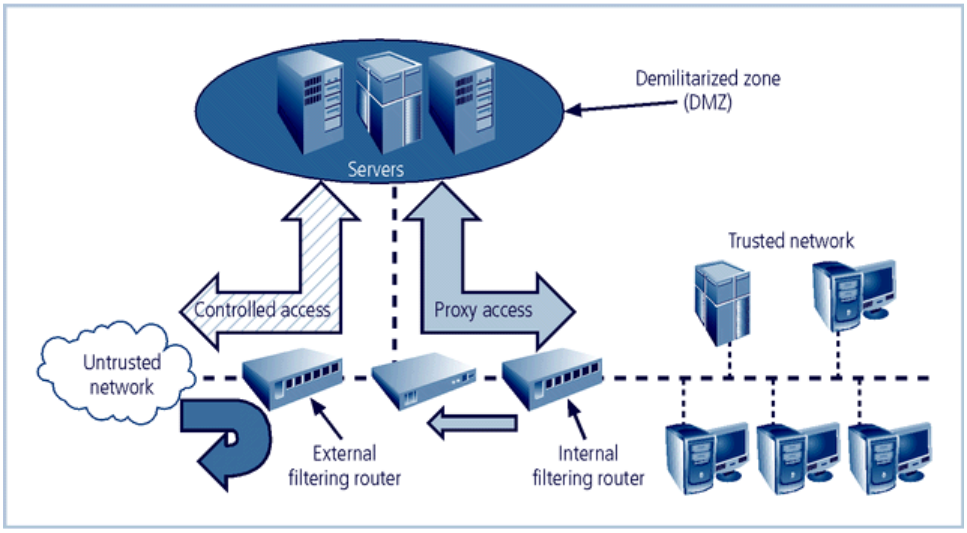



**FIGURE 8-5** Screened Subnet (DMZ)

**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

## 2. 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

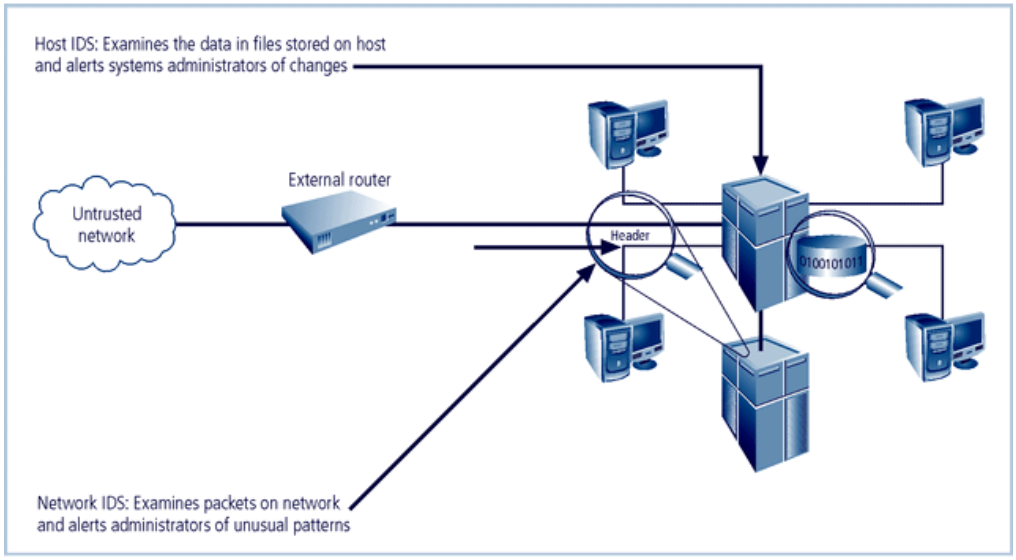



**FIGURE 8-7** Intrusion Detection Systems

## Types of IDSs

### a) Network-based IDS

A network-based IDS(NIDS) resides on a computer or an appliance connected to a segment of an organization's network and monitors traffic on that network
Segment, looking for indications of ongoing or successful attacks.

- 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).
  - To detect attack ,NIDS look for attack patterns.
  - This is implemented by using special implementation of TCP/IP stack.
  - NIDs looks for invalid data packets.
  - Both host-and network based IDSs require a database of previous activity.

**Advantages of NIDS**

- Good network design and placement of NIDS can enable organization to use a few devices to monitor large network**.**
- NIDs are usually passive and can be deployed into existing networks with little disruption to normal network operations.
- NIDs not usually susceptible to direct attck and may not be detectable by attackers.

**Disadvantages of NIDs:**

- They can become overwhelmed by network volume and fail to recognize attacks.
- They require access to all traffic to be monitored.
- It cannot analyze encrypted packets.
- They cannot reliably ascertain if attack was successful or not
- Some forms of attack are nor easily discerned by NIDs, specifically those involving fragmented packets.

**b) <u>Host-based IDS</u>**

**A** Host-based IDS(HIDS) works differently from a network-based version of IDS. While a netwerok-based-IDS resides on a network segment and monitors activities across that segment,

a host-based IDS resides on a particular computer or server, known as the host and monitors activity only on that system.

HIDs are also known as **System Integrity Verifiers** as they benchmark and monitor the status of key system files and detect when an intruder creates ,modifies or deletes monitored files.

A HIDs is also capable of monitoring system configuration databases, such as windows registries in addition to stored configuration files like .ini,.cfg,and .dat files.

**Advantages of HIDS:**

- This can detect local events on host systems and detect attacks
- The functions on host systems, where encrypted traffic will have been decrypted and is available for processing.
- They are not affected by use of switched network protocols.
- They can detect inconsistencies in how applications and systems programs were used by examining records stored in audit logs.

**Disadvantages of HIDS:**

- They pose more management issues
- It is vulnerable both to direct attacks and attacks against host operating system.
- It does not detect multi host scanning or scanning of non-host network devices.
- They are susceptible to some denial of service attacks

**c) Application-based IDS**

A refinement of Host-based IDs is the application-based IDS(AppIDS). Whereas the HIDs examines a single system for file modification, the application based IDs examines an application for abnormal incidents. It looks for anomalous occurrences such as users exceeding their authorization, invalid file executions etc.

**d) Signature-based IDS**

It is based on detection methods. A signature-based IDS(also called Knowledge-based IDs) examines data traffic in search of patterns that match known signatures – that is, preconfigured ,predetermined attack patterns.

Many attacks have clear and distinct signatures such as

(i) foot printing and fingerprinting activities, have an attack pattern that includes the use of ICMP,DNS querying, and e-mail routing analysis

(ii) Exploits involve a specific attack sequence designed to take advantage of a vulnerability to gain access to a system (iii) Denial of Service(DoS) and Distributed Denial of Service(DDoS) attacks.

**e) Statistical Anomaly-Based IDS(Also called Behaviour-based IDS)**

- This approach is used for detecting intrusions based on the frequency with which certain network activities takes place.
- **Statistical Anomaly-Based IDS** collects statistical summaries by observing traffic that is known to be normal.

- The Stats IDs periodically sample network activity, and using statistical methods ,compares the sampled network activity to the baseline.
- When the measured activities are outside the baseline parameters,it is said to be exceeding the **clipping level**;at this point, the IDS will trigger an alert to notify the administrator.

**f) Log File Monitors(LFM)**

Log File Monitor(LFM) is an approach to IDS that is similar to NIDS. Using LFm the system reviews the log files generated by servers,network devices,and wven other IDSs. 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.

**3. SCANNING AND ANALYSIS TOOLS**

- 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
- Scanning tools collect information about the attackers and help to trap them.
- One of the preparatory parts of an attack is known as footprinting – 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

**Port scanners**

- A Port Scanner is a software application designed to probe a server or host for open ports.
- Port scanners fingerprint networks to find ports and services and other useful information.
- This is often used by the administrators to verify security policies of their networks and by attackers running services on a host.
- 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 scanner is a computer program designed to assess computers, computer systems, networks or applications for weaknesses.
- 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
- Using the information captured by the packet sniffer, an administrator can identify erroneous packets and help to maintain efficient data transmission.
- 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**)**

Packet sniffing can be generally termed as **Employee Monitoring**

**Content Filters**

- The content filtering restricts web sites with inappropriate content.
- Content filters act either on the content, the information contained in the mail body, or on the mail headers to either classify, accept or reject a message
- Although technically not a firewall, a content filter is a software filter that allows administrators to restrict accessible content from within a network
- Restriction of websites and non business related materials from entering inside the network is called as **Pornography.**

**Trap and Trace**

- The trap describes the software designed with a view to entice the individuals who are illegally invading inside the network.
- The invaders will always work towards the rich content areas of the network.
- These are known as honey pots and they distract the attacker while notifying the administrator
- **Trace**: determine the identity of someone using unauthorized access

- Better known as honey pots, they distract the attacker while notifying the administrator
- If the person is internal to the organization then the administrators could easily track each of their activity.
- If the person is external to the organization then the organization can go for legal measures.

## 4.CRYPTOGRAPHY AND ENCRYPTION BASED SOLUTIONS

**Cryptography** ,which comes from the Greek work kryptos,meaning "hidden",and graphein, meaning "to write",is aprocess of making and using codes to secure the transmission of information.

**Cryptoanalysis** is the process of obtaining the original message(called **plaintext**) from an encrypted message(called the **ciphertext**) 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**.**
- **Ciphertext 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 ciphertext to plaintext**.**
- **Encipher**: to encrypt or convert plaintext to ciph**ertext.**

- **Key or cryptovariable: the information used in conjunction with the algorithm to create ciphertext from plaintext.**
- **Keyspace:** 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**.**
- **Block cipher method :**The message is divided into blocks, i.e 8 or 16 bit then each block is transformed using the algorithm and key.

**Encryption Operations**

- In encryption the most commonly used algorithms include two functions:

Substitution , transposition.

- In substitution cipher ,we substitute one value for another.
- This type of substitution is based on a Monoalphabetic substitution , since it only uses one alphabet.
- More advanced substitution ciphers use two or more alphabets and are referred to as polyalphabetic substitution.

**Vernam Cipher**

- Also known as one time pad. the vernam cipher uses a one use set of characters,the value is added to the block of text.
- The resulting sum is then converted to text.
- When the two are added, if the values exceed 26,26 is subtracted from the total (Modulo 26)-the corresponding results are then converted back to text.

**Book or Runnign key Cipher**

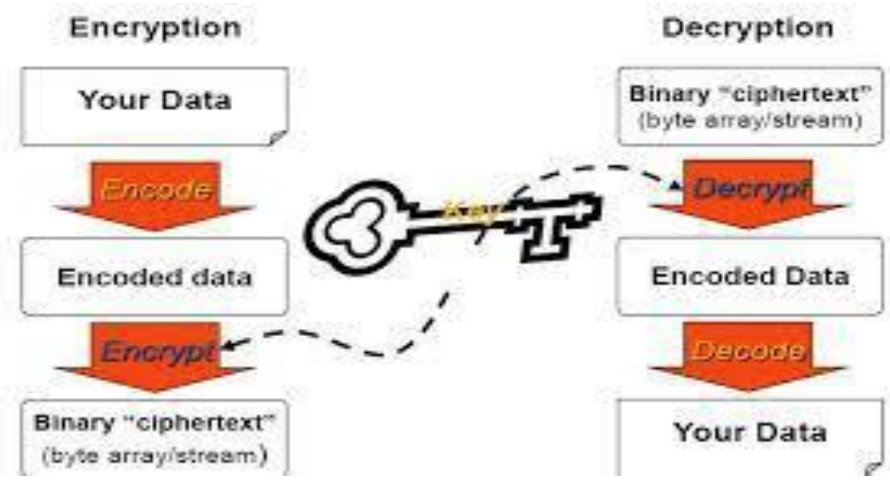
Another method ,made popular by spy movies, is the use of text in a book as the Algorithm to decrypt a message .

The key consists of

- Knowing which room to use
- A list of codes representing the page number, line number, and word number of the plaintext word

**Symmetric Encryption**

- This uses same secret key to encipher and decipher message .
- Encryption methods can be extremely efficient,requiring minimal processing.
- Both sender and receiver must possess the encryption key .
- Symmetric key encryption can use either stream ciphers or block ciphers.




**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)

**Algorithm steps :**

**1).Initial Permutation**:

The Plaintext block undergoes an initial permutation.64 bits of the block are permuted

**2) A complex Transformation**:

64 bit permuted block undergoes 16 rounds of complex transformations.

**3) 32 bit swap:**

32 bit left and right halves of the output of the $16^{th}$ round are swapped.

**4).Inverse Initial Permutation**:

The 64 bit output undergoes a permutation that is inverse of the initial permutation. The 64 bit output is the ciphertext.

**Details of function F:**

- It takes 32 bits input and produces a 32 bit output.32 bit input is expanded into 48 bits. This is done by permuting and duplicating some bits of 32 bits
- Ex-OR operation is performed between these 48 bits and 48 bit subkey.
- 48 bit output of the Exclusive OR operation is grouped into 8 groups of 6 bits each.
- Each 6 bit group is fed into a 6 to 4 substitution box that transforms 6 bits to 4 bits.
- 32 bit output of the permutation box is F(Ri-1,Ki)

**Triple DES (3DES)**

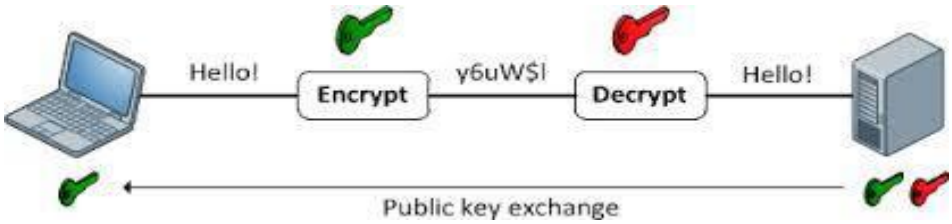
- Developed as an improvement to DES
- Uses up to three keys in succession and also performs three different encryption operations:
  - 3DES encrypts the message three times with three different keys, the most secure level of encryption possible with 3DES
- In 1998, it took a dedicated computer designed 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

**Advanced Encryption standard. (AES)**

- The advanced encryption standard was published by NIST(National Institute of Standards and Technology ) in 2001.
- AES is a symmetric block cipher that is intended to replace DES as the approved standard for a wide range of applications.
- This is a replacement for DES because Triple-DES is slow, has small blocks.
- AES is a private key symmetric block cipher with 128 bit data and 128/192/256 bit keys.

**Asymmetric Encryption**

- In the public key systems or asymmetric encryption, two keys are used.
- Anyone knowing the public key can encrypt messages or verify signatures,but cannot decrypt messages or create signatures.
- Asymmetric encryption involves the use of two keys.:
  - A public key, which may be known to anybody, and can be used to encrypt messages and verify signature.
  - A private key known only to the recipient used to decrypt messages, and sign (create)signatures.




**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 **nonrepudiation**, which is the foundation of digital signatures

- **Digital Signatures** are encrypted messages that are independently verified by a central facility (registry) as authentic.
- A **digital signature** or digital signature scheme is a mathematical scheme for demonstrating the authenticity of a digital message or document.

**RSA(Rivest –shamir-Aldeman)**

- This is the best known and widely used public key scheme.
- Each user generates a public/privare key pair by :
- selecting two large primes at random p,q
- computing their system modulus N=p.q
- Select the encryption key e, where $1 < e < \emptyset(n)$,$\gcd(e, \emptyset(N)) = 1$
- Solve the following equation to find decryption key d,
  - e.d=1 $mod\ \emptyset(N) and\ 0 \leq d \leq N$
- The public encryption key key :KU=$\{e, N\}$ and the secret private decryption key: KR=$\{d, p, q\}$
- The public key of of recipient KU=$\{e, N\}$ and computes: C=M.e mod N,
  - where $0 \leq M \leq N$.
- To decrypt the ciphertext C the owner uses their private key KR=$\{d, p, q\}$ and computes :M=Cd mod N.

**Public key Infrastructure (PKI)**

PKI 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).

Common implementations of PKI include:

- systems to issue digital certificates to users and servers;
- encryption enrollment;
- key issuing systems;
- tools for managing the key issuance;
- verification and return of certificates; and any other services associated with PKI.

PKI protects information assets in several ways:

♦ **Authentication**: Digital certificates in a PKI system permit individuals, organizations, and Web servers to validate the identity of each of the parties in an Internet transaction.

♦ **Integrity**: A digital certificate demonstrates that the content signed by the certificate has not been altered while being moved from server to client.

♦ **Privacy:** Digital certificates keep information from being intercepted during transmission over the Internet.

♦ **Authorization**: Digital certificates issued in a PKI environment can replace user IDs and passwords, enhance security, and reduce some of the overhead required for authorization processes and controlling access privileges for specific transactions.

♦ **Non-repudiation**: Digital certificates can validate actions, making it less likely that customers or partners can later repudiate a digitally signed transaction, such as an online purchase.

**Digital certificates:**

A digital certificate is an electronic document, similar to digital signature, attached to a file certifying that this file is from the organization it claims to be from and has not been modified from the original format.

**Securing E-mail**

- Encryption cryptosystems have been adapted to inject some degree of security into e-mail:
  - S/MIME builds on the Multipurpose Internet Mail Extensions (MIME) encoding format by adding encryption and authentication
  - Privacy Enhanced Mail (PEM) was proposed by the Internet Engineering Task Force (IETF) as a standard to function with the public key cryptosystems
  - PEM uses 3DES symmetric key encryption and RSA for key exchanges and digital signatures
  - Pretty Good Privacy (PGP) was developed by Phil Zimmerman and uses the IDEA Cipher along with RSA for key exchange

## Securing the Web

**Secure electronic Transaction** (SET) :SET is a system for ensuring the security of financial transaction on the internet

**Secure Socket Layer**: SSL is a commonly used protocol for managing the security of a message transmission on the internet

**Secure Hypertext transfer Protocol(SHTTP)** :S-HTTP provides a wide variety of mechanisms to provide for confidentiality, authentication, and integrity.

**Secure Shell (SSH)** :SSH is a network protocol for secure data communication, remote shell services or command execution and other secure network services between two networked computers that it connects via a secure channel over an insecure network.

**IPSEC(IP Security) :**IP security is the cryptographic authentication and encryption product used to create virtual private networks and is an open framework for security development within the TCP /IP family of protocol standards.

## Securing Authentication

- Kerberos is a symmetric key encryption method to secure authentication.

- Kerberos uses symmetric key encryption to validate an individual user to various network resources.
- Kerberos keeps and database containing the private keys of clients and servers, which, in the case of a client is the client's encrypted password.

The Kerberos system knows these private keys and can authenticate one network node (client or server) to another for example, Kerberos can authenticate a client to a print service. To understand Kerberos, think of a friend introducing you around at a party. Kerberos also generates temporary session keys, which are private keys given to the two parties in a conversation. The session key is used to encrypt all communications between these two parties.

Kerberos consists of three interacting services all using a data base library:

1. Authentication server (AS), which is a Kerberos server that authenticates clients and servers.
2. Key Distribution Center (KDC), which generates and issues session keys.
3. Kerberos ticket granting service (TGS), which provides tickets to clients who request services.

- In Kerberos a **ticket** is an identification card for a particular client that verifies to the server that the client is requesting services and that the client is a valid member of the Kerberos system and therefore authorized to receive services.
- The ticket consists of the client's name and network address, a ticket validation starting and ending time, and the session key, all encrypted in the private key of the server from which the client is requesting services.

Kerberos works based on the following principles:

"The KDC knows the secret keys of all clients and servers on the network. "The KDC initially exchanges information with the client and server by using these secret keys. "Kerberos authenticates a client to a requested service on a server through TGS and by issuing temporary session keys for communications between the client and KDC, the server and KDC, and the client and server. "Communications then takes place between the client and server using these temporary session keys."

(1) User logs into client machine (c)

(2) Client machine encrypts password to create client key (Kc)

(3) Client machine sends clear request to Kerberos tgs

(4) Kerberos tgs returns ticket consisting of :

## 5. ACCESS CONTROL DEVICES

- To insure secure operation, access control needs strong authentication.
- Consists of the users personal password or passphrase but requires at least one other factor to represent strong authentication.
- Frequently a physical device is used for the second factor.

When considering access control you address:

- What you know
- What you have
- Who you are
- what you produce

**What you know**

This deals with passwords , passphrase or any other unique authentication code.

A **password** is a private word or combination of characters that only one person ought to know.

The password should be complex (i.e) difficult for others to guess.

A **passphrase** is similar to passwords but longer than passwords from which a virtual password could be retrieved.

**What you have**

- These include **dumb cards,** such as ID cards or ATM cards with magnetic stripes containing the digital (and often encrypted) user personal identification number (PIN) against which a user input is compared.

- A better version is the **smart card,** which contains a computer chip that can verity and validate a number of pieces of information above and beyond the PIN Another device often used is the token, a computer chip in a display that presents a number used to support remote login authentication. Tokens are synchronous or asynchronous.

- Once **synchronous tokens** are synchronized with a server, each device (server and token) uses the time or a time-based database to generate a number that is entered during the user login phase. **Asynchronous tokens** use a challenge- response system, in which the server challenges the user during login with a numerical sequence. The user places this sequence into the token and receives a response.

**What You Are**

This involves the entries area of biometrics discussed earlier. Biometrics includes:

- Fingerprints
- Palm scan
- Hand geometry
- Hand topology
- Keyboard dynamics
- ID cards (face representation)
- Facial recognition

- Retina scan
- Iris scan
- Voice recognition

With all these metrics, only three human characteristics are considered truly unique:

- Fingerprints
- Retina of the eye (blood vessel pattern)
- Iris of the eye (random pattern of features found in the rise including: freckles, pits, striations, vasculature, coronas, and crypts)

**Figure Recognition Characteristics**

- Most of the technologies that scan human characteristics convert these images to some form of minutiae.
- **Minutiae** are unique points of reference that are digitized and stored in an encrypted format.
- Each subsequent scan is also digitized and then compared with the encoded value to determine if users are whom they claim to be.

The problem is that some human characteristics can change over time, due to normal development, injury, or illness.

**What You Do**

- The fourth and final area of authentication addresses something the user performs or something they produce.

- This includes technology in the areas of signature recognition and voice recognition, or at least signature capture, for authentication during a purchase.

- The customer signs his or her signature on a special pad, with a special stylus that captures the signature. The signature is digitized and either simply saved for future reference, or compared to a database for validation.

- Currently, the technology for signature capturing is much more widely accepted than that for signature comparison, because signatures change over time due to a number of factors,

including age, fatigue, and the speed with which the signature is written. Voice recognition works similarly. There are several voice recognition software packages on the market today. These monitor the analog waveforms of a human's speech and attempt to convert them into on – screen text.

- Voice recognition for authentication is much simpler, as the captured and digitized voice is only compared to a stored version for authentication, rather than for text recognition. Systems that use voice recognition provide the user with a phrase that they are expected to read. This phrase is then compared to a stored version for authentication, for example, "My voice is my password, please verify me. Thank you.

**Effectiveness of Biometrics**

Biometric technologies are evaluated on three basic criteria: first,

- The false reject rate, :which is the percentage of authorized users that are denied access;
- The false accept rate, which is the percentage of unauthorized users allowed access;
- The crossover error rate, which is the point at which the number of false rejections equals the false acceptances.

**False Reject Rate**

The false **reject rate** is the percentage or value associated with the rate at which authentic users are denied or prevented access to authorized areas, as a result of a failure in the biometric device.

This error rate is also known as a Type 1 error.

**False Accept Rate**

The **false accept rate** is the percentage or value associated with the rate at which fraudulent or nonusers are allowed access to systems or areas as a result of a failure in the biometric device.

This error rate is also knows as a Type II error.

This type of error is unacceptable to security, as it represents a clear breach of security.

.

**Cross over Error Rate (CER)**

The **cross over error rate** is the point at which the number of false rejections equals the false acceptances, also known as the equal error rate.

This is possibly the most common and important overall measure of the accuracy of a biometric system.

Most biometric systems can be adjusted to compensate for both false positive and false negative errors.

Adjustment to one extreme creates a system that requires perfect matches and results in high false rejects, but almost no false accept. Adjustment to the other extreme allows low false rejects, but produces high false accept.

## 6. PHYSICAL SECURITY

### 6.1 ACCESS CONTROLS

There are a number of physical access controls that are uniquely suited to the physical entry and exit of people to and from the organization's facilities. Some times the technology of physical security control can overlap logical security control technologies. Some of these overlaps include biometrics, smart cards, or wireless enabled keycards, which are used for controlling access to locked doors, information assets, and information system resources

**Secure Facility**

- 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

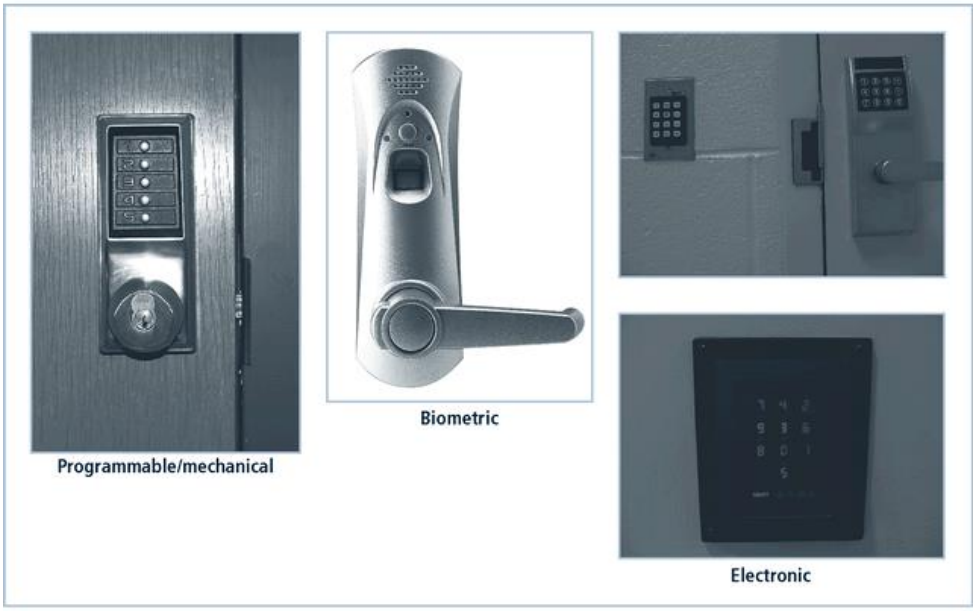
**ID Cards and Badges**

- 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




Biometric image courtesy of the BioThentica Corporation

**FIGURE 9-1** Locks

## 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

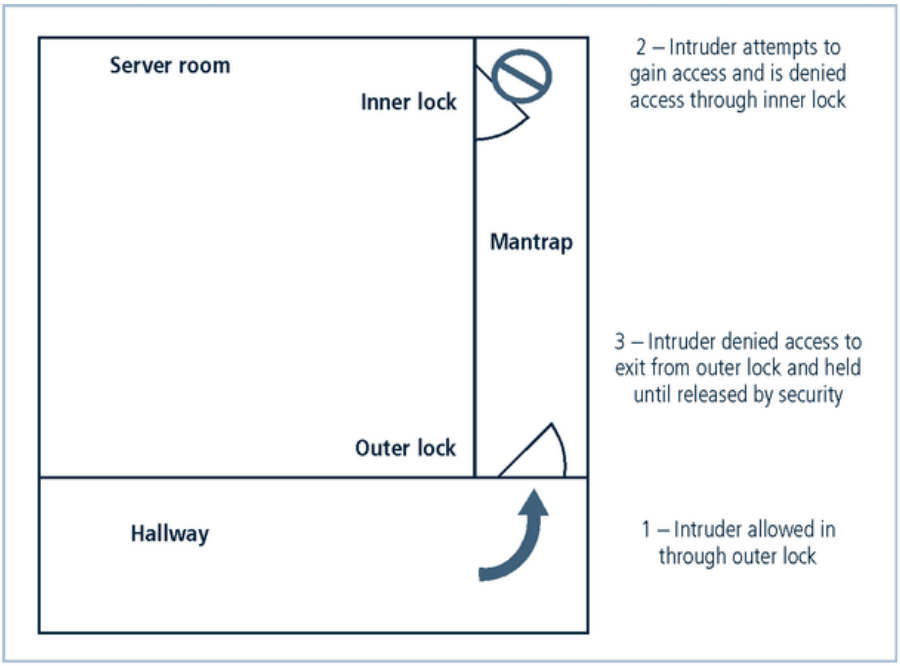



**FIGURE 9-2** Mantraps

## Electronic Monitoring

- 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

## 6.2 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

**Fire detection**

Fire detection systems fall into two general categories:

manual and automatic.

**Manual fire detection systems**

include human responses, such as calling the fire department, as well as manually activated alarms, such as sprinklers and gaseous systems. When manually triggered alarms are tied directly to suppression systems, as false alarms are not uncommon. During the chaos of a fire evacuation, and attacker can easily slip into offices and obtain sensitive information. There are three basic types of fire detection systems: thermal detection, smoke detection, and flame detection.

The **thermal detection systems :**

contain a sophisticated heat sensor that operates in one of two ways. In the first, known as **fixed temperature,** the sensor detects when the ambient temperature in an area reaches a predetermined level, usually between 235 degrees Fahrenheit and 165 degrees Fahrenheit, and 165 degrees Fahrenheit, or 57 degrees Centigrade to 74 degrees Centigrade. In the second, known as **rate-of-rise,** the sensor detects an usually rapid increase in the area temperature, within a relatively short period of time.

**Smoke detection systems** are perhaps the most common means of detecting a potentially dangerous fire, and they are required by building codes in most residential. Smoke detectors operate in one of three ways.

In the first, **photoelectric sensors** project and detect an infrared beam across an area. If the beam is interrupted (presumably by smoke), the alarm or suppression system is activated.

In the second, an **ionization sensor** contains a small amount of a harmless radioactive material within a detection chamber. When certain by-products of combustion enter the chamber, they change the level of electrical conductivity with the chamber and activate the detector.

The third category of smoke detectors is the air-aspirating detector. **Air-aspirating detectors** are very sophisticated systems, which are used in high-sensitivity areas.

The third major category of fire detection systems is the **flame detector.**

The flame detector is a sensor that detects the infrared or ultraviolet light produced by an open flame. These systems require direct line of sight with the flame and compare the flame "signature" to a database to determine whether or not to activate the alarm and suppression systems.

**Fire Suppression**

Fire suppression systems can consist of portable, manual, or automatic apparatus. Portable extinguishers are used in a variety of situations where direct application of suppression is preferred, or fixed apparatus is impractical.

Portable extinguishers are much more efficient for smaller fires, because they avoid the triggering of an entire building's sprinkler systems and the damage that can cause. Portable extinguishers are rated by the type of fire they can combat as described below.

**Class A:** Fires that involve ordinary combustible fuels such as wood, paper, textiles, rubber, cloth, and trash. Class A fires are extinguished by agents that interrupt the ability of the fuel to be ignited. Water and multipurpose, dry chemical fire extinguishers are ideal for these types of fires.

**Class B:** Fires fueled by combustible liquids or gases, such as solvents, gasoline, paint, lacquer, and oil. Class B fires are extinguished by agents that remove oxygen from the fire. Carbon dioxide, multipurpose dry chemical and halon fire extinguishers are ideal for these types of fires.

**Class C:** Fires with energized electrical equipment or appliances. Class C fires are extinguished with agents that must be nonconducting.
Carbon dioxide, multipurpose, dry chemical, and halon fire extinguishers are ideal for these types of fires. Never use a water fire extinguisher on a Class C fire.

**Class D:** Fires fueled by combustible metals, such as magnesium, lithium, and sodium. Fires of this type require special extinguishing agents and techniques."

All **sprinkler systems** are designed to apply liquid, usually water, to all areas in which a fire has been detected. In sprinkler systems, the organization can implement wet-pipe, dry-pipe, or pre-action systems.

A **wet-pipe** system has pressurized water in all pipes and has some form of valve in each protected area. When the system is activated, the valves are opened allowing water to sprinkle the area.

A **dry-pipe** system is designed to work in areas where electrical equipment is used. Instead of the system containing water, it contains pressurized air. The pressurized air holds valves closed. Keeping the water away from the target areas. The pressurized air holds valves closed, keeping the water away from the target areas. When a fire is detected and the sprinkled heads are activated, the pressurized air escapes, water fills the pipes, and exits through the sprinkler heads.

A third type of sprinkler system is the **pre-action system.** Unlike either the wet-or dry-pipe systems, the pre-action system has a two-phase response to a fire. The system is normally maintained with nothing in the delivery pipes. When a fire has been detected, the first phase is initiated, and valves allow water to enter the system. The second phase is to intimate the responsible individuals

**Gaseous Emission systems**:

Major types of gaseous systems: **carbon dioxide** and **halon**. Carbon dioxide robs a fire of its oxygen supply. Halon is one of a few chemicals designated as a **clean agent,** which means that it does not leave any residue when dry, nor does it interfere with the operation of electrical or electronic equipment. Unlike carbon dioxide, halon does not rob the fire of its oxygen and produces instead a chemical reaction with the flame to extinguish it. As a result it is much safer than carbon dioxide when people are present and the system is activated. These alternative clean agents include the following.

FM-200 (very similar to halon 1301) is safe in occupied areas

 Inergen is a high-pressure agent composed of nitrogen, argon and carbon dioxide

 Carbon dioxide, although riskier than halon, is an acceptable alternative.

 FE-13 (trifluromethane) is one of the newest and safest clean agent variations of the most commonly used clean agents and ensure no one is left behind. It is also important to have fire suppression systems see Figure, which are both manual and automatic, inspected and tested regularly.

## 7. SECURITY AND PERSONNEL

- When Implementing information security there are many human resource issues that must be addressed:
  - Positioning and naming
  - Staffing
  - Evaluating impact of information across every role in IT function.
  - Integrating solid information security concepts into personnel practices.
- Employing often threatened when organization is creating or enhancing overall information security program.

### Positioning and staffing the security function

- The security function can be placed within :
  - IT function
  - Physical security function
  - Administrative services function
  - Insurance and risk management function
  - Legal department
- Organizations must balance needs of enforcement with needs for education, training , awareness, and customer service.

### Staffing the Information security function

- Selecting personnel is based on many criteria, including supply and demand.
- Many professionals enter security market by gaining skills, experience, and credentials.
- At present ,information security industry is in period of high demand.

**Qualifications and Requirements:**

- The following factors must be addressed while dealing with Qualifications and Requirements:
    - Management should learn more about position requirements and qualifications.
    - Upper management should learn about budgetary needs of information security function
    - IT and management must learn more about level of influence and prestige ,the information security function should be given to be effective.
- Organizations typically look for technically qualified information professionals who understand.
    - How an organization operates at all levels.
    - Information security usually a management/problem,not a technical problem.
    - Strong communications and writing skills.
    - The role of policy in guiding security efforts.
    - Most mainstream IT technologies.
    - The terminology of IT and information security.

**Entry into the Information security Profession**

- Many information security professionals enter the field through one of two career paths:
    - Law enforcement and military.
    - Technical,working on security applications and processes.
- Today ,students select and and trailer degree programs to prepare for work in information security.
- Organizations can foster greater professionalism by matching candidates to clearly defined expectations and position descriptions.

**Information Security positions**

Use of standard job description can increase degree of professionalism and improve the consistency of roles and responsibilities between organization.

Charles Cresson Wood's book and Responsibilities made easy offers set of model job description.

**a) Chief Information Security Officer (CISO or CSO)**

- Top Information security position; frequently reports to chief Information Officer.
- Manages the overall information security program.
- Drafts or approves information security policies.
- Works with the CIO on strategic plans
- Develops information security budgets.
- Sets priorities for information security projects and technology.
- Makes recruiting ,hiring and firing decisions or recommendations.
- Acts as spokesperson for information security team.
- Typical qualifications: accreditation; graduate degree; experience

b) **Security Manager**

- Accountable for day-to-day operation of information security program.
- Accomplish objectives as identified by CISO.
- Typical qualifications: not uncommon to have accreditation; ability to draft middle and lower level policies, standards and guidelines; budgeting ,project management, and hiring and firing ;manage technicians.

**c) Security Technician**

Technically qualified individuals tasked to configure security hardware and software

Typical qualification:

-Varied: organization prefer expert, certified, proficient technician

-Some experience with a particular hardware and software package.

- Actual experience in using a technology usually required.