

Topic 04

Information

Security ***BBA II***

Learning Objectives

Upon completion of this lecture, you should be able to:

- Understand what information security is all about
- Understand the need for information security.
- Understand the threats posed to information security and the more common attacks associated with those threats.

Information security defined

- Information security, is the practice of defending information from unauthorized
 - *Access, Use, Disclosure, Disruption, Modification, Inspection, Recording or destruction.*
- Computer Security refers to protecting computer systems and the information they contain against unwanted access, damage, modification or destruction.
- Information security protects both the **systems** that keep the information and the **information its self**.
- The ability of the computer system to protect information and system resources such as CPU, disks, programs

ELEMENTS OF INFORMATION SECURITY

- Information security has three main elements i.e.



- Confidentiality:** Protects information from unauthorized disclosure and safeguards privacy.
- Integrity:** Prevents unauthorized users from creating, modifying, or deleting information.
- Availability:** Ensures that authorized users have timely and reliable access to necessary information.

Other elements of information security

- **Privacy;** Information is to be used only for purposes known to the data owner.
- **Identification;** Identification and authentication are essential to establishing the level of access or authorization that an individual is granted.
- **Authentication;** occurs when a control provides proof that a user possesses the identity that he or she claims.
- **Authorization;** authorization provides assurance that the user has been specifically & 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.

Need For Information Security

- Information security performs four important functions for an organization:
 - **Protects the data the organization collects and uses**
 - *Most valuable asset*
 - *Without data organization lose records of transaction*
 - **Safeguards the technology assets in use at the organization**
 - *Organizations must have secure infrastructure services based on the size and scope of the enterprise*
 - **Protects the organization's ability to function**
 - *Information security breaches can have significant impact and cost on organizations*
 - Enables the safe operation of applications implemented on the organization's IT systems

Threats

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

Management must be informed of the various kinds of threats facing the organization.

This helps management to effectively protect its information through:

- ***Policy,***
- ***Education and training, and***
- ***Technology controls***



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 of 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 from service providers	Power and WAN service issues
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

Acts of Human Error or Failure

- Includes acts done without malicious intent
- Caused by:
 - ***Inexperience***
 - ***Improper training***
 - ***Incorrect assumptions***
 - ***Other circumstances***
- Employees are greatest threats to information security – They are closest to the organizational data

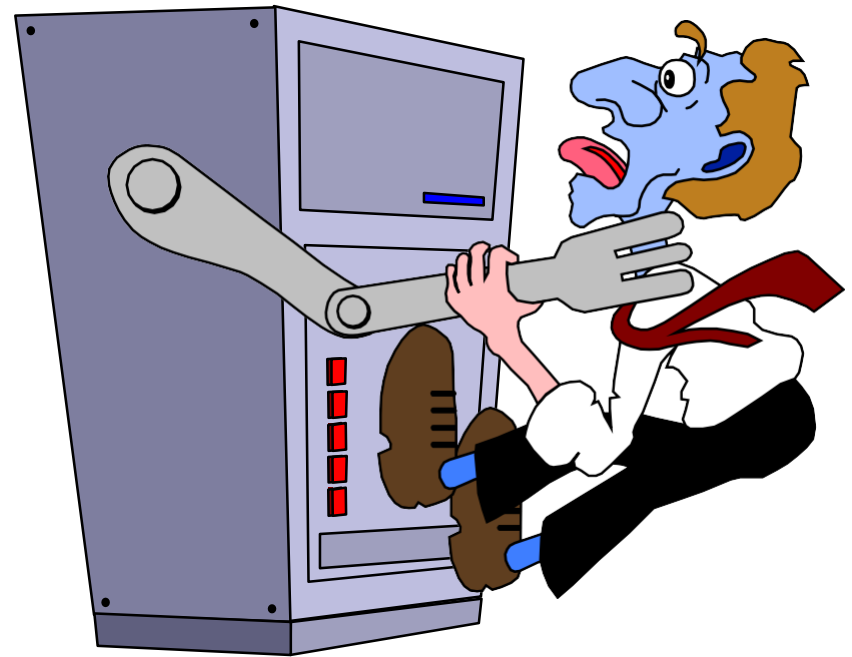


Acts of Human Error or Failure

■ Employee mistakes can easily lead to the following:

- ***revelation of classified data***
- ***entry of erroneous data***
- ***accidental deletion or modification of data***
- ***storage of data in unprotected areas***
- ***failure to protect information***

■ Many of these threats can be prevented with controls



Who is the biggest threat to your organization?



Tom Twostory
convicted burglar



Dick Davis a.k.a.
"wannabe amateur hacker"



Harriet Allthumbs
Employee
accidentally
deleted the one copy
of a critical report

FIGURE 2-1 Acts of Human Error or Failure

Deviations in Quality of Service by Service Providers

- Situations of product or services not delivered as expected.
- Information system depends on many inter-dependent support systems.
- Three sets of service issues that dramatically affect the availability of information and systems are
 - ***Internet service***
 - ***Power irregularities***
 - ***Communications***

Espionage/Trespass

- Broad category of activities that breach confidentiality

- Unauthorized accessing of information
- Competitive intelligence vs. espionage
- Shoulder surfing can occur any place a person is accessing confidential information

- Controls implemented to mark the boundaries of an organization's virtual territory giving notice to trespassers that they are encroaching on the organization's cyberspace

- Hackers uses skill, guile, or fraud to steal the property of someone else





Shoulder surfing
takes many forms.
Some may not be obvious.



FIGURE 2-2 Shoulder Surfing



Traditional hacker profile:
Age 13-18, male with limited
parental supervision spends all his
free time at the computer



Modern hacker profile:
Age 12-60, male or female, unknown
background, with varying technological
skill levels; may be internal or external
to the organization

FIGURE 2-3 Hacker Profiles

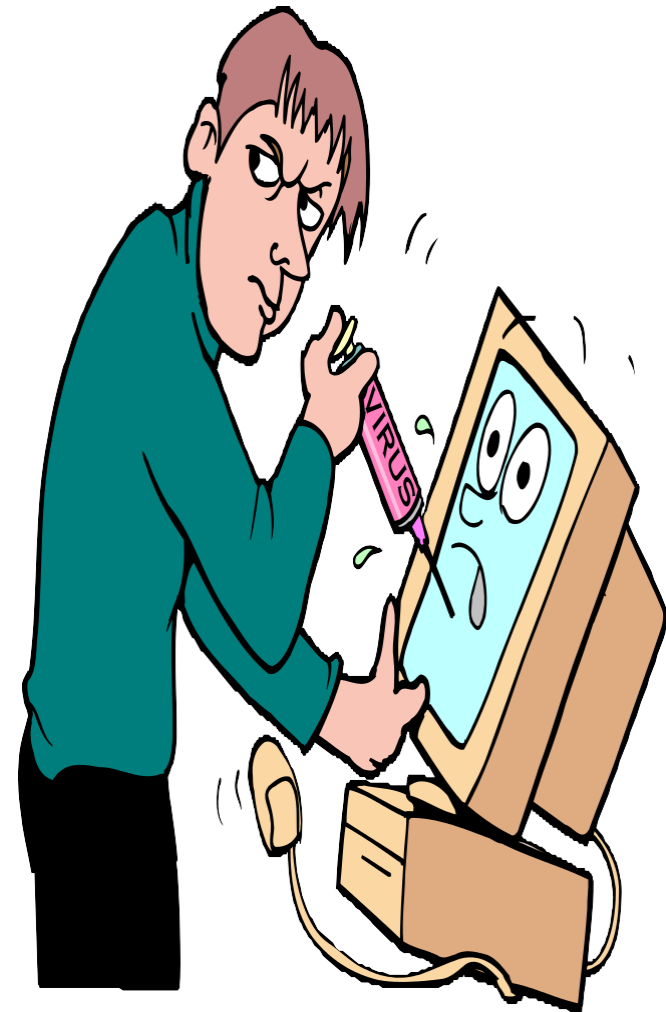
Information Extortion

- Information extortion is an attacker or formerly trusted insider stealing information from a computer system.
- They tend to demand compensation for its return or non-use.
- Extortion found in credit card number theft



Sabotage or Vandalism

- Individual or group who want to deliberately sabotage the operations of a computer system or business, or organization
- They perform acts of vandalism to either destroy an asset or damage the image of the organization
- These threats can range from petty vandalism to organized sabotage
- The most extreme version is cyber-terrorism



Deliberate Acts of Theft

- Illegal taking of another's property - physical, electronic, or intellectual

- ***The value of information suffers when it is copied and taken away without the owner's knowledge***

- Physical theft can be controlled - a wide variety of measures used from locked doors to guards or alarm systems.
- Electronic theft is a more complex problem to manage and control - organizations may not even know it has occurred

Deliberate Software Attacks

- When an individual or group designs software to attack systems, they create malicious code/software called malware

- ***Designed to damage, destroy, or deny service to the target systems***

- Includes:
 - macro virus
 - boot virus
 - worms
 - Trojan horses
 - logic bombs
 - backdoors
 - denial-of-service attacks



Deliberate Software Attacks

- **Virus** is a computer program that attaches itself to an executable file or application.
- It can replicate itself, usually through an executable program attached to an e-mail.
- **Denial-of-service:** Attacker sends a large number of information requests to a target system.
- **A worm** is a computer program that replicates and propagates itself without having to attach itself to a host.
- **Backdoors** are computer programs that give attackers a means of regaining access to the attacked computer later.
- **Trojan Programs** disguise themselves as useful computer programs or applications and can install a backdoor on a computer.

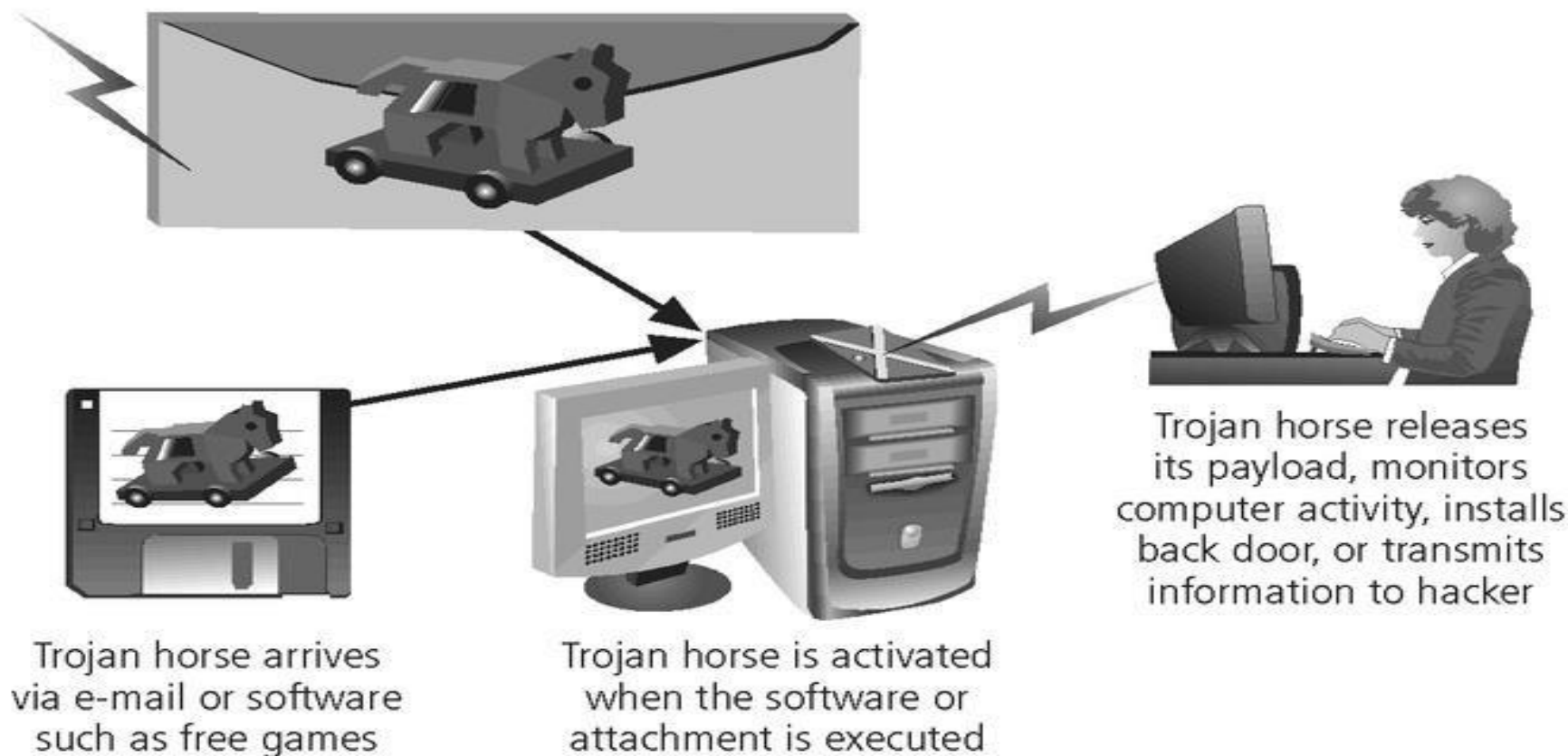


FIGURE 2-8 Trojan Horse Attack

Compromises to Intellectual Property

- Intellectual property is “the ownership of ideas and control over the tangible or virtual representation of those ideas”
- Many organizations are in business to create intellectual property
 - trade secrets
 - copyrights
 - trademarks
 - patents

Forces of Nature

- Forces of nature or acts of God are dangerous because they are unexpected and can occur with very little warning.
- Can disrupt not only the lives of individuals, but also the storage, transmission, and use of information. They include:
 - ***fire,***
 - ***flood,***
 - ***earthquake,***
 - ***lightning***
 - ***volcanic eruption and insect infestation***
- Since it is not possible to avoid many of these threats, management must implement controls to limit damage and also prepare contingency plans for continued operations

Technical Hardware Failures or Errors

- Technical hardware failures or errors occur when a manufacturer distributes to users equipment containing flaws
- These defects can cause the system to perform outside of expected parameters, resulting in unreliable service or lack of availability
- Some errors are terminal, in that they result in the unrecoverable loss of the equipment
- Some errors are intermittent, in that they only periodically manifest themselves, resulting in faults that are not easily repeated

Technological Obsolescence

- When the infrastructure becomes outdated, it leads to unreliable and untrustworthy systems.
- Management must recognize that when technology becomes outdated, there is a risk of loss of data integrity to threats and attacks.
- Ideally, proper planning by management should prevent the risks from technology obsolescence, but when obsolescence is identified, management must take action

WAYS/METHODS OF ENSURING COMPUTER SECURITY (SECURITY MEASURES)

- **Physical security/Access Control**; describes measures that prevent or deter attackers from accessing a facility, resource, or information stored on physical media. It can be as simple as a locked door or a gate with spikes on top.

There are four **layers of physical security**:

Environmental Design: this is the initial layer of security for physical space to deter threats. E.g. barbed wire, warning signs and fencing.

Mechanical; second layer is and includes gates, doors, and locks. Keys quickly become unmanageable forcing the adoption of electronic access control.

WAYS/METHODS OF ENSURING COMPUTER SECURITY (SECURITY MEASURES)

layers of physical security:

Intrusion detection: third layer is systems or alarms. Intrusion detection monitors for attacks. It is less a preventative measure and more of a response measure, although it can work as a deterrent.

Video monitoring systems: Like intrusion detection, are not much of a deterrent. Video monitoring systems are more useful for incident verification and historical analysis.

WAYS/METHODS OF ENSURING COMPUTER SECURITY (SECURITY MEASURES)

- **Identification and Authentication;** a control that provides proof that a user possesses the identity that he or she claims. A credential is used for Authentication e.g. providing a PIN (Personal Identification Number), access card (e.g. including magnetic stripe, bar code, smart cards), or biometric feature (fingerprint, facial recognition, iris recognition, retinal scan, voice, and hand geometry), Digital signatures.
- **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 & explicitly authorized by the proper authority to access, update, or delete the contents of an information asset.

WAYS/METHODS OF ENSURING COMPUTER SECURITY (SECURITY MEASURES)

- **Audit/accountability;** every user of the system or information is monitored and the changes effected by the user noted for accountability to provide assurance that every activity undertaken can be attributed to a named person or automated process. Accountability uses system components like Audit trails and logs.
- **Encryption;** this is a measure where information or data is coded (scrambled) so that it makes sense to only the people that it is intended for. Normal text is converted into cipher text and the key sent to the recipient to decipher (decode) the text back to normal text.
- **Software Firewalls;** this is a software that is installed in the computer network to study and moderate the network traffic coming in to the network. All data coming in to the organization is first checked for authenticity and viruses before penetrating the network.

WAYS/METHODS OF ENSURING COMPUTER SECURITY (SECURITY MEASURES)

- **Centralized Enterprise Anti-virus system;** an anti-virus is installed in the server computer and all computers in the network are scanned for viruses and cleaned using a centralized enterprise anti-virus. The anti-virus can be installed in stand alone computers for individuals to scan their computers.
- **Passwords;** they are the most common tool for restricting access to computer systems. They are only effective when chosen carefully, Do not choose a password that is easy to crack. They should be between four and eight letters (alphabetic or numeric). Some security systems refuse to allow users to choose any real words as passwords. They should be changed frequently (e.g. monthly).
- **Backup;** any complete security system must have some plan for recovering from disaster. All information should be backed up and the back up copy preferably kept off sight.

WAYS/METHODS OF ENSURING COMPUTER SECURITY (SECURITY MEASURES)

- **Protection from fire;** security should be ensured from fires and arsonist attacks by using sprinklers, carbondioxide gas fire extinguishers, smoke detectors, fire alarms, fireproof material for construction like paint, train fire fighters, exit roots.
- **Protection from water and floods;** place computers and storage devices on elevated structures, water proof ceiling and floors, good drainage system, avoid placing drinks and food near computers etc.
- **Protection from Lightening and electrical outages;** use Uninterruptible Power Supply (UPS), stand by generators, Lightening arrestors etc.
- **Security from Heat;** Install good ventilations for aeration, air conditioners, open windows or doors etc.
- **Security from dust;** cover the computers and peripherals when not in use. Occasionally blow the equipment to clean them from dust.

RISK MANAGEMENT: Information Systems Security

INTRODUCTION

- In the real world, ***absolute*** security is not a realistic goal.
- Instead, managers must balance the ***value of the assets being protected, potential risks*** to the organization, and ***security costs***.
 - ***For example, it might not be worth installing an expensive video camera monitoring system to protect an empty warehouse.***
- To achieve the best results, most firms use a **risk management** approach

Risk Management

- From information systems security perspective, risk management is the process of identifying, assessing and controlling risks facing an organization's information systems and the data kept in them.
- **Risk identification:** Process of examining an organization's assets, potential threats and vulnerabilities that may affect the organization.
- **Risk assessment:** It measures the risk likelihood and impact the risk will have on the organization in case it happened .
- **Risk control:** Applying controls to reduce risks and their impact to an organizations information and information systems.

RISK IDENTIFICATION

It also involves identifying the potential threats to an organizations information system and the data in it.

- The first step in risk identification is to list and classify business assets. An **asset** might include company
 - *hardware, software,*
 - *data,*
 - *networks,*
 - *people, or procedures.*
- For each asset, a risk manager rates the impact of an attack and analyses possible threats.
- A **threat** is an internal or external entity that could endanger an asset.
- For example, threat categories might include natural disasters, software attacks, or theft

RISK IDENTIFICATION

THREAT	CATEGORY
Extortion	Hacker steals trade secrets and threatens to release them if not paid.
Hardware and software failures	Router stops functioning, or software causes the application server to crash
Human error or failure	Employee accidentally deletes a file from the computer
Natural disasters	Flood destroys company building and networked systems.
Service failure	Electricity is disrupted and brings the entire system down for hours.
Software attack	A group plants destructive software, a virus, or a worm into a company network.
Trespass and espionage	Employee enters unlocked server room and views the payroll data on a forbidden system.
Vandalism	Attacker defaces Web site logo, or destroys CEO's hard drive physically or electronically.

RISK IDENTIFICATION

- Next, the risk manager identifies **vulnerabilities** and how they might be **exploited**.
- A **vulnerability** is a security weakness or soft spot.
- **Exploit** is an attack that takes advantage of a vulnerability.
- To identify vulnerabilities, a risk manager might ask questions like these:
 - ***Could hackers break through the proxy server?***
 - ***Could employees retrieve sensitive files without proper authorization?***
 - ***Could people enter the computer room and sabotage our servers?***
- Each vulnerability is rated and assigned a value.
- The output of risk identification is a list of assets, vulnerabilities, and ratings.

Risk identification

Assets	Vulnerability	Rating
Offices	No security personnel deployed	High
Computer Labs	Unlocked computer labs	High
Network connection	Lack of firewalls installed	Medium
Server room	Unlocked server rooms	High
Information system	Lack of permission to sensitive files on the system	High

RISK IDENTIFICATION

Risks can be identified by:

- Brainstorming with key employees who have knowledge of the department processes
- Discussing risks with professionals like risk managers and auditors
- Making judgments based on experience
- Employing systems analyst,

RISK ANALYSIS

- Analysis or assessment basically looks at the probability of occurrence of a risk and impact it will have on an asset of the organization.
 - ***This involves looking at the risks identified and estimating the likelihood of their occurrence in the context of existing control measures***
- The consequences of particular risks also need to be considered.
- The aim of this assessment is to separate the ***minor*** acceptable risks from ***major*** risks
 - *The outcome of risk analysis provides the basis for protection planning.*
 - Normally low probability and low effect risks might be assessed and accepted, monitored and periodically reviewed.
 - High risks should be prioritized and treated

Risk Assessment

Problematic Event or Incident	Probability of occurrence	Impact Classification & Effect on finances, legal liability, human life, reputation
Fire	Low	Crisis, at times Major, Human life
Hacking Attack	High	Major, Legal liability
Network Unavailable	High	Crisis
Social engineering, /Fraud	High	Major, Legal liability
Server Failure (Disk/server)	Medium	Major, at times: Crisis

Considerations in risk analysis

- Investigate the frequency of particular types of disasters
- Determine the degree of predictability of the disaster
- Analyse the speed of the disaster (sudden vs gradual)
- Estimate the duration of the disaster
- Consider the impact of the disaster on vital records

TREAT THE RISK

- This phases of risks management involves:
 - *Identifying the range of options for treating risks.*
 - *Evaluating options on the basis of the extent of the benefits and costs of implementing the options.*

Treatment of risks may involve:

- Implementing protective measures such as:
 - *We could place a firewall on the proxy server;*
 - *We could assign permissions to sensitive files;*
 - *We could install biometric devices to guard the computer room.*
- **Prevention is the first line of defense against risk**
 - *Prevention measures are designed to minimize the likelihood of damage to systems from one or more threats*

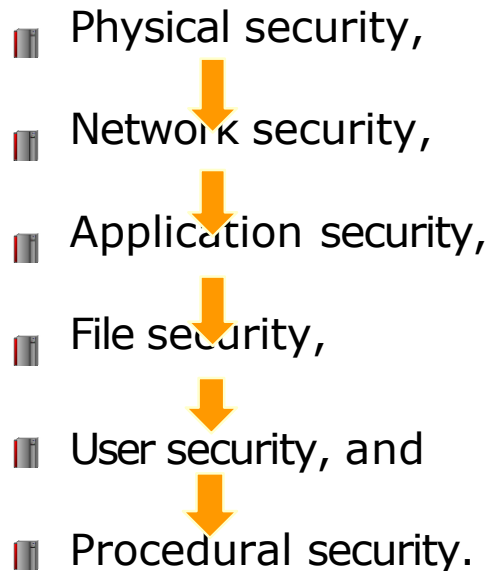
Risk control strategies

■ Typically, management chooses one of four risk control strategies:

- **Avoidance** eliminates the risk by adding protective safeguards. ***For example, to prevent unauthorized access to LAN computers, a secure firewall might be installed.***
- **Mitigation** reduces the impact of a risk by careful planning and preparation. ***For example, a company can prepare a disaster recovery plan in case a natural disaster occurs.***
- **Transference** shifts the risk to another asset or party, such as an insurance company.
- **Acceptance** means that nothing is done. Companies usually accept a risk only when the protection clearly is not worth the expense..

Security Levels

- To provide system security, you must consider six separate but interrelated levels:



NOTE:

Each security link has a specific focus, and the overall chain is only as strong as the weakest link.

Physical Security

- The first level of system security concerns the physical environment, including IT resources and people throughout the company.
- Special attention must be paid to critical equipment located in operations centers, where servers, network hardware, and related equipment operate.
- Large companies usually have a dedicated room built specifically for IT operations. Smaller firms might use an office or storage area.

Physical security

- Regardless of its size and shape, an operations center requires special protection from unwanted intrusion.
- In addition to centrally located equipment, all computers on the network must be secure, because each server or workstation can be a potential access point.
- Physical access to a computer represents an entry point into the system and must be controlled and protected.

Physical Security Measures

- Using electromagnetic locks
- Installing **biometric scanning systems**,
- Video cameras and motion sensors can be used to monitor computer room security
- Equipping desktop computers and servers with locks
- **power-on password**,

Network security

- It looks at protecting network traffic that is been exchange between devices that are connected on a computer network.
- To provide security for network traffic, data can be **encrypted**, which refers to a process of encoding the data so it cannot be accessed without authorization.
- **ENCRYPTING NETWORK TRAFFIC** Network traffic can be intercepted and possibly altered, redirected, or recorded. For example, if an **unencrypted**, or **plain text**, password or credit card number is transmitted over a network connection, it can be stolen.
- When the traffic is encrypted, it still is visible, but its content and purpose are masked.
- **FIREWALLS:** A **firewall** is the main line of defense between a local network, or intranet, and the Internet.
- Firewall software examines all network traffic sent to and from each network interface.
- **NETWORK INTRUSION DETECTION:** Suppose an intruder attempts to gain access to the system an intrusion alarm should be sounded when certain activity or known attack patterns are detected.

File security

- Computer configuration settings, users' personal information, and other sensitive data are stored in files.
- The safety and protection of these files is a vital element in any computer security program.
- A systems analyst needs to consider the importance of encryption, or encoding files to make them unreadable by unauthorized users.
- There is also need to assign permissions, to individual users or to user groups so as to assign certain files in the system.
- **ENCRYPTION:** It scrambles the contents of a file or document to protect it from unauthorized access.
- This is especially important for sensitive material such as personnel or financial records.
- **PERMISSIONS:** These describe the rights a user has to a particular file or directory on a server.
- The most common permissions are read, write, and execute.

User security

- User security involves the identification of system users and consideration of user-related security issues.
- Regardless of other security precautions and features, security ultimately depends on system users and their habits, practices, and willingness to support security goals.
- Unfortunately, many system break-ins begin with a user account that is compromised in some way. *User security requires*
 - **identity management,**
 - **comprehensive password protection,**
 - **an effective means of overcoming user resistance,**
- **Identity management:** Refers to controls and procedures necessary to identify legitimate users and system components.
- **Password protection:** As the section on physical security points out, a secure system must have a password policy that requires minimum length, complexity, and a limit on invalid login attempts.
- **Constant awareness and training:** Many users, including some senior managers, dislike tight security measures because they can be inconvenient and time consuming so there need to constantly remind them of the importance of security

Procedural/ Operational security

- It is concerned with managerial policies and controls that ensure secure operations.
 - ***security depends more on managerial issues than technology.***
- Management must work to establish a corporate culture that stresses the importance of security to the firm and its people.
- Procedural security defines how particular tasks are to be performed, from large-scale data backups to everyday tasks such as storing e-mails or forms.
- Other procedures might spell out how to update firewall software or how security personnel should treat often to change password
- Procedural security also includes safeguarding certain procedures that would be valuable to an attacker