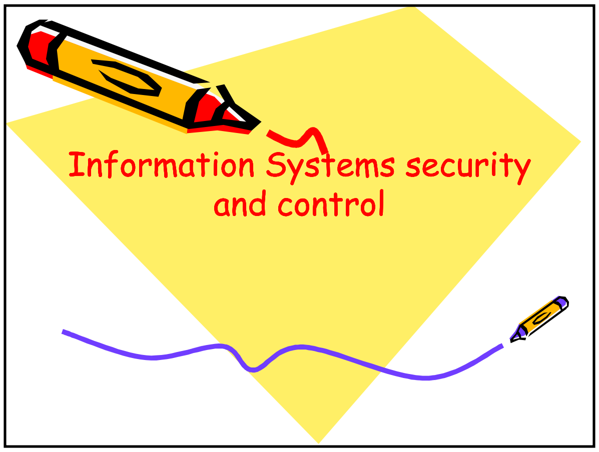
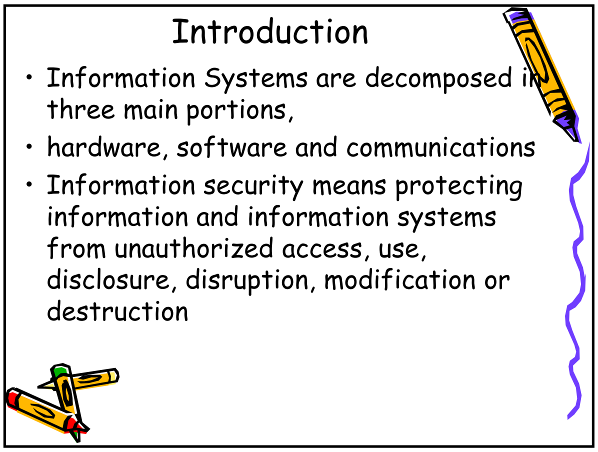
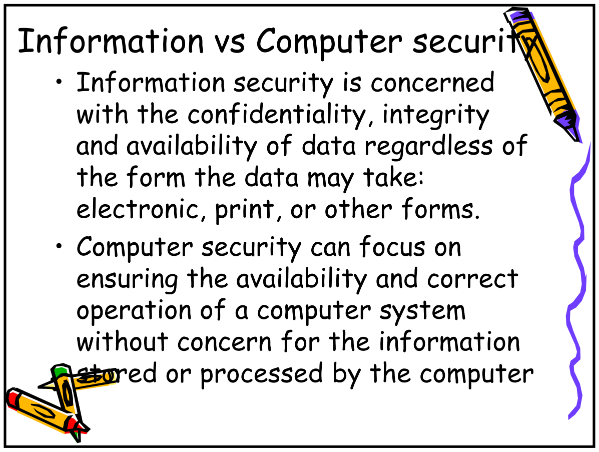


Information Systems security and control



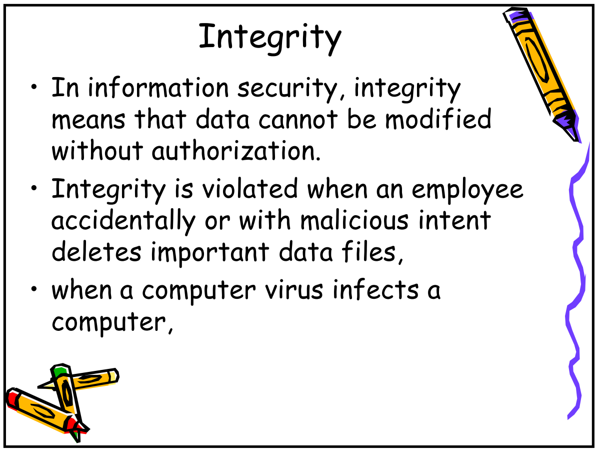
Introduction

- Information Systems are decomposed in three main portions,
- hardware, software and communications
- Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction



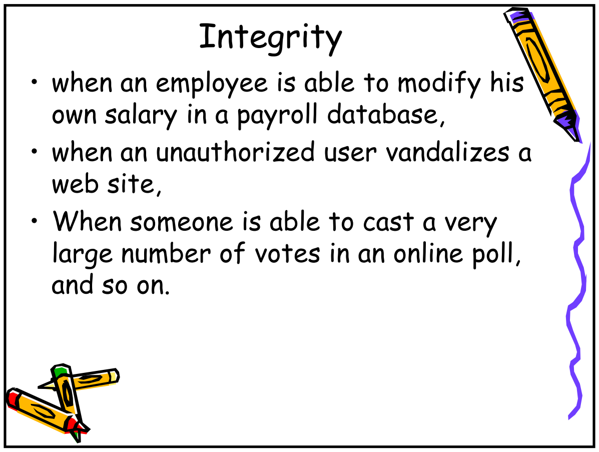
Information vs Computer security

- Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms.
- Computer security can focus on ensuring the availability and correct operation of a computer system without concern for the information stored or processed by the computer



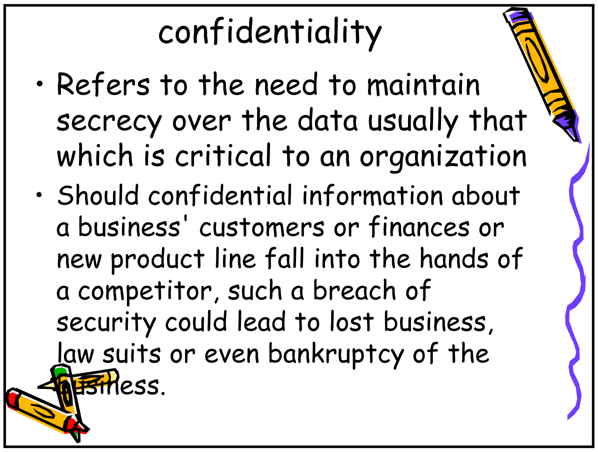
Integrity

- In information security, integrity means that data cannot be modified without authorization.
- Integrity is violated when an employee accidentally or with malicious intent deletes important data files,
- when a computer virus infects a computer,



Integrity

- when an employee is able to modify his own salary in a payroll database,
- when an unauthorized user vandalizes a web site,
- When someone is able to cast a very large number of votes in an online poll, and so on.



confidentiality

- Refers to the need to maintain secrecy over the data usually that which is critical to an organization
- Should confidential information about a business' customers or finances or new product line fall into the hands of a competitor, such a breach of security could lead to lost business, law suits or even bankruptcy of the business.

Availability

- Data must be available to authorized persons at an appropriate time (when as required)
- Loss leads to the inability to access data.
- Ensuring availability also involves preventing denial-of-service attacks.

Security controls

- Security controls are measures taken to safeguard an information system from attacks against the confidentiality, integrity, and availability (C.I.A.) of the information system

Security Control Types

- Security controls are categorized in three different types.
  - Administrative controls
  - Logical controls
  - Physical controls

Administrative controls

- Administrative controls (also called procedural controls) consist of
  - Approved written policies, procedures, standards and guidelines
- Administrative controls form the framework for running the business and managing people.
- They inform people on how the business is to be run and how day to day operations are to be conducted.

Administrative controls

- Laws and regulations created by government bodies are also a type of administrative control because they inform the business.
- Examples of administrative controls include the corporate security policy, password policy, hiring policies, and disciplinary policies.

Logical controls

- Logical controls (also called technical controls) use software and data to monitor and control access to information and computing systems.
- For example: passwords, network and host based firewalls, network intrusion detection systems, access control lists, and data encryption are logical controls.

Logical controls

- An important logical control that is frequently overlooked is the principle of least privilege.
- The principle of least privilege requires that an individual, program or system process is not granted any more access privileges than are necessary to perform the task.

Physical controls

- Physical controls monitor and control the environment of the work place and computing facilities.
- They also monitor and control access to and from such facilities.
- For example: doors, locks, heating and air conditioning, smoke and fire alarms, fire suppression systems, cameras, barricades, fencing, security guards, cable locks, etc.
- Separating the network and work place into functional areas are also physical controls.

Security Control Types

- second way to categorize security controls is taxonomy based on
- what the control does (verb) (that is, direct, prevent, correct).
- The common categories for this taxonomy are directive, preventive, detective, corrective, and recovery security controls.

Preventive, Detective, Corrective, and Recovery Security Controls

- Preventive security controls are put into place to prevent intentional or unintentional disclosure, alteration, or destruction (D.A.D.) of sensitive information.
- Some example preventive controls follow:
  - Policy – Unauthorized network connections are prohibited.
  - Firewall – Blocks unauthorized network connections.
  - Locked wiring closet – Prevents unauthorized equipment from being physically plugged into a network switch.

Detective security controls

- They are like a burglar alarm.
- They detect and report an unauthorized or undesired event (or an attempted undesired event)
- Example
  - detective security controls are log monitoring and review, system audit, file integrity checkers, and motion detection

Corrective security controls

- They are used to respond to and fix a security incident.
- Corrective security controls also limit or reduce further damage from an attack.
- Examples:
  - Procedure to clean a virus from an infected system
  - A guard checking and locking a door left unlocked by a careless employee
  - Updating firewall rules to block an attacking IP address

Recovery security controls

- They are those controls that put a system back into production after an incident.
- Most Disaster Recovery activities fall into this category.
  - For example, after a disk failure, data is restored from a backup tape.

Other Security Control Types

- Directive security controls
  - They are the equivalent of administrative controls.
  - Directive controls direct that some action be taken to protect sensitive organizational information.
  - The directive can be in the form of a policy, procedure, or guideline.

Deterrent security controls

- They are controls that discourage security violations.
  - For instance, "Unauthorized Access Prohibited" signage may deter a trespasser from entering an area.
  - The presence of security cameras might deter an employee from stealing equipment.
  - A policy that states access to servers is monitored could deter unauthorized access.

Compensating security controls

- They are controls that provide an alternative to normal controls that cannot be used for some reason.
  - For instance, a certain server cannot have antivirus software installed because it interferes with a critical application.
  - A compensating control would be to increase monitoring of that server or isolate that server on its own network segment.

Application Controls

- specific controls unique to each computerized application, such as payroll or order processing.
- They consists all controls applied from the business functional area of a particular system and from programmed procedures.
- Classifications of application controls are:

Application Controls

- **Input controls**: the procedures to check data for accuracy and completeness when they enter the system.
- **Processing controls**: the routines for establishing that data are complete and accurate during updating.
- **Output controls**: measures that ensure that the results of computer processing are accurate, complete and properly distributed

TECHNOLOGIES AND TOOLS FOR SECURITY AND CONTROL

- Authorization
- Authentication
- Encryption
- Digital Signature
- Firewalls
- Intrusion Detection Systems
- Antivirus

Authorization

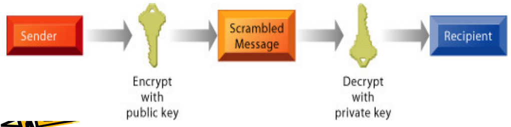
- Also known as Access control
  - This is the granting of rights and privileges that enables a user to have access to the system

Authentication:

- Mechanisms that determines whether a user is s/he what s/he claims to be
- Establishing proof of identity
  - Physical traits
  - Pin codes
  - Cards etc
  - Passwords

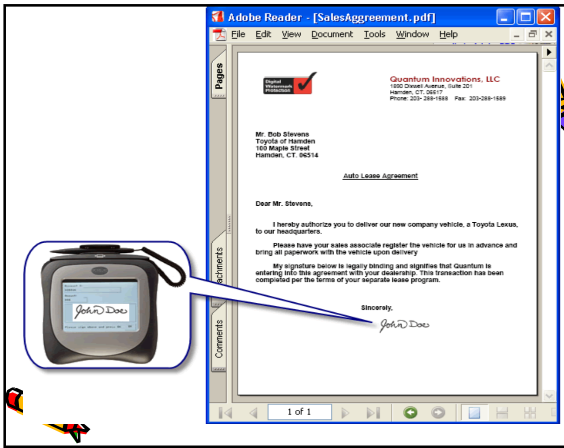
Encryption

- This is the encoding of the data by a special algorithm that renders the data unreadable by any program without the decryption key.



Digital signature

- Digital signatures are a way of authenticating the identity of creators or producers of digital information.
- A digital signature is like a handwritten signature and can have the same legal authority in certain situations,
- Digital signatures can also be used to ensure that the information signed has not been tampered with during transmission or repudiated after being received.



Quantum Innovations, LLC
1890 Dixwell Avenue, Suite 201
Hamden, CT. 06517
Phone: 203- 288-1588 Fax: 203-288-1589

Mr. Bob Stevens
Toyota of Hamden
100 Maple Street
Hamden, CT. 06514

Auto Lease Agreement

Dear Mr. Stevens,

I hereby authorize you to deliver our new company vehicle, a Toyota Lexus, to our headquarters.

Please have your sales associate register the vehicle for us in advance and bring all paperwork with the vehicle upon delivery

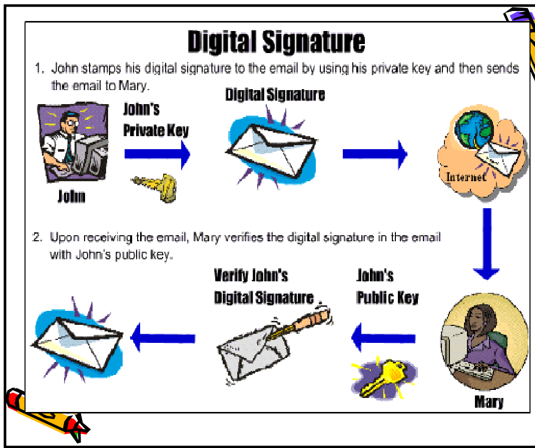
My signature below is legally binding and signifies that Quantum is entering into this agreement with your dealership. This transaction has been completed per the terms of your separate lease program.

Sincerely,

John Doe

Digital Signature

1. John stamps his digital signature to the email by using his private key and then sends the email to Mary.



2. Upon receiving the email, Mary verifies the digital signature in the email with John's public key.

Firewalls

- Hardware and software controlling flow of incoming and outgoing network traffic
- What this means is that if you browse to a web site, the firewall will allow the traffic to reach your computer.
- On the other hand, if you did not request information from that web site, and the web site sent traffic to you, it would be denied from reaching your computer

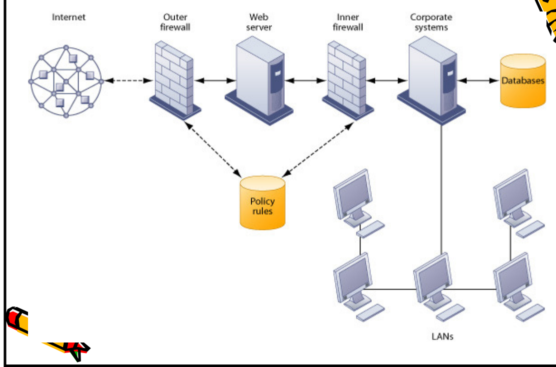
Hardware and software firewalls

- A Hardware Firewall is a device that sits between your Internet connection and the rest of the computers plugged into it.
- These firewalls usually come with a built in hub that allows you to connect multiple computers to it in order for them all to be able to share one Internet connection

Hardware and software firewalls

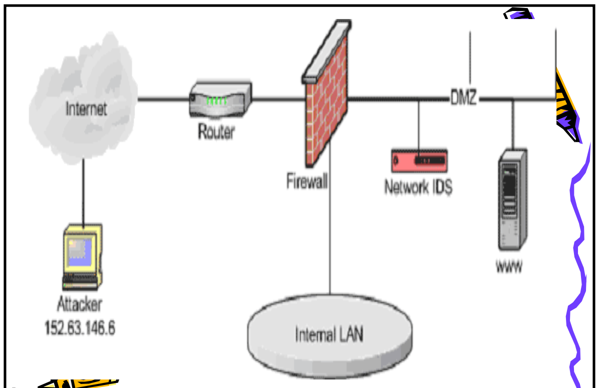
- A Personal Firewall is a piece of software installed on each computer that needs to be protected.
- This software then filters all incoming, and sometimes outgoing traffic, and only allows only data that has been requested or explicitly allowed to pass through

A Corporate Firewall



Intrusion Detection Systems

- Full-time monitoring tools placed at the most vulnerable points of corporate networks to detect and deter intruders



Antivirus Software

- Software that checks computer systems and drives for the presence of computer viruses and can eliminate the virus from the infected area