IT Security and Risk Management

Information Security

ا.د. حنان الطاهر الداقيز

h.dagez@uot.edu.ly

ربيع 2024

https://t.me/+xavNMXu7DyM5Yjc0

What is Information Security?

- means protecting information and information systems from unauthorised access, use, disclosure, modification or destruction.

or

- Implementing suitable controls - policies, practices, procedures, organisational structures, software, etc, to secure information for any information user.

What is Information Security?

- **Information security** in today's enterprise is "well informed sense of assurance that the information risks and control are in balance
- **Security** is a non functional requirement assumes that the system is correctly implemented according to functional requirement.
- Security **is a process** not a product

Security Types

- Data security
  - **Data security** is the means of ensuring that data is kept safe from corruption and that access to it is suitably controlled.
- Computer Security
  - The objective of computer security includes protection of information and property from theft, corruption, or natural disaster, Malware: malicious software
    - includes computer viruses, worms, Trojan horses,,

Network Security

- protect the network and the network-accessible resources from unauthorized access, consistent and continuous monitoring and measurement of its effectiveness

Why we need computer security?

- Why the need for Computer Security?
  - The value of computer assets and services
- What is the new IT environment?
  - Networks and distributed applications/services
  - Electronic Commerce (E-commerce, E-business)

Terminology

- Vulnerabilities : i) Weakness in a security system.
  ii) "Vulnerability" refers to the security flaws in a system that allow an attack to be successful.
  crack in wall or wall is short in height.
- Threats : i) Set of circumstances that might exploit vulnerability
  ii) "threat" refers to the source and means of a particular type of attack
  Overflow of water, wall may be break
- Attacks : i) When weakness is exploited
  Actually breaking of wall.

Vulnerability, threat and controls

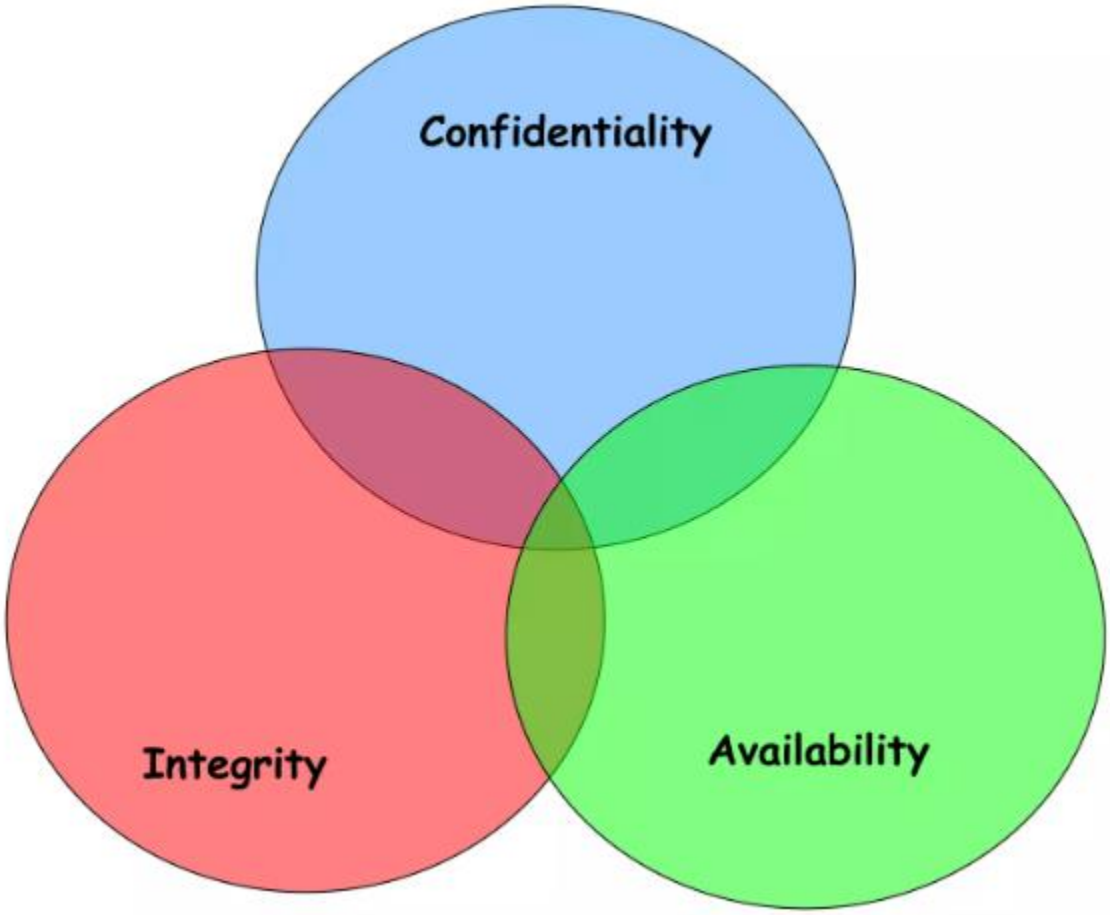
A **vulnerability** is a weakness in the security system, for example, in procedures, design, or implementation, that might be exploited to cause loss or harm.

A **threat** to a computing system is a set of circumstances that has the potential to cause loss or harm.

A *threat* is blocked by *control of* a *vulnerability*.

"Ensures that only authorized users (confidentiality) have access to accurate and complete information (integrity) when required (availability)

Information Security Goals



Information Security Goals

- Confidentiality - making sure that those who should not see the information can not see it.
- Integrity - making sure the information has not been changed from how it was intended to be.
- Availability – making sure the information is available for use when needed.

Confidentiality

- Secrecy requires that the information in a computer system only be accessible for reading by authorized parties.
- This type of access includes:
  - Printing
  - Displaying
  - Other forms of disclosure,

Integrity

- Integrity requires that the computer system asset can be modified only by authorized parties.
- Modification includes:
  - Writing
  - Changing
  - Changing status
  - Deleting and
  - Creating

Availability

- Availability requires that computer system assets are available to authorized parties.
- Availability is a requirement intended to assure that systems work promptly and service is not denied to authorized users.

Authenticity

- Authenticity means that parties in a information services can ascertain the identity of parties trying to access information services.
- Also means that the origin of the message is certain.
- Receiver should be ensure about sender's identity, that false sender(imposter) should has not sent the message

Accountability

- Accountability is an essential part of an information security plan. The phrase means that every individual who works with an information system should have specific responsibilities for information assurance.

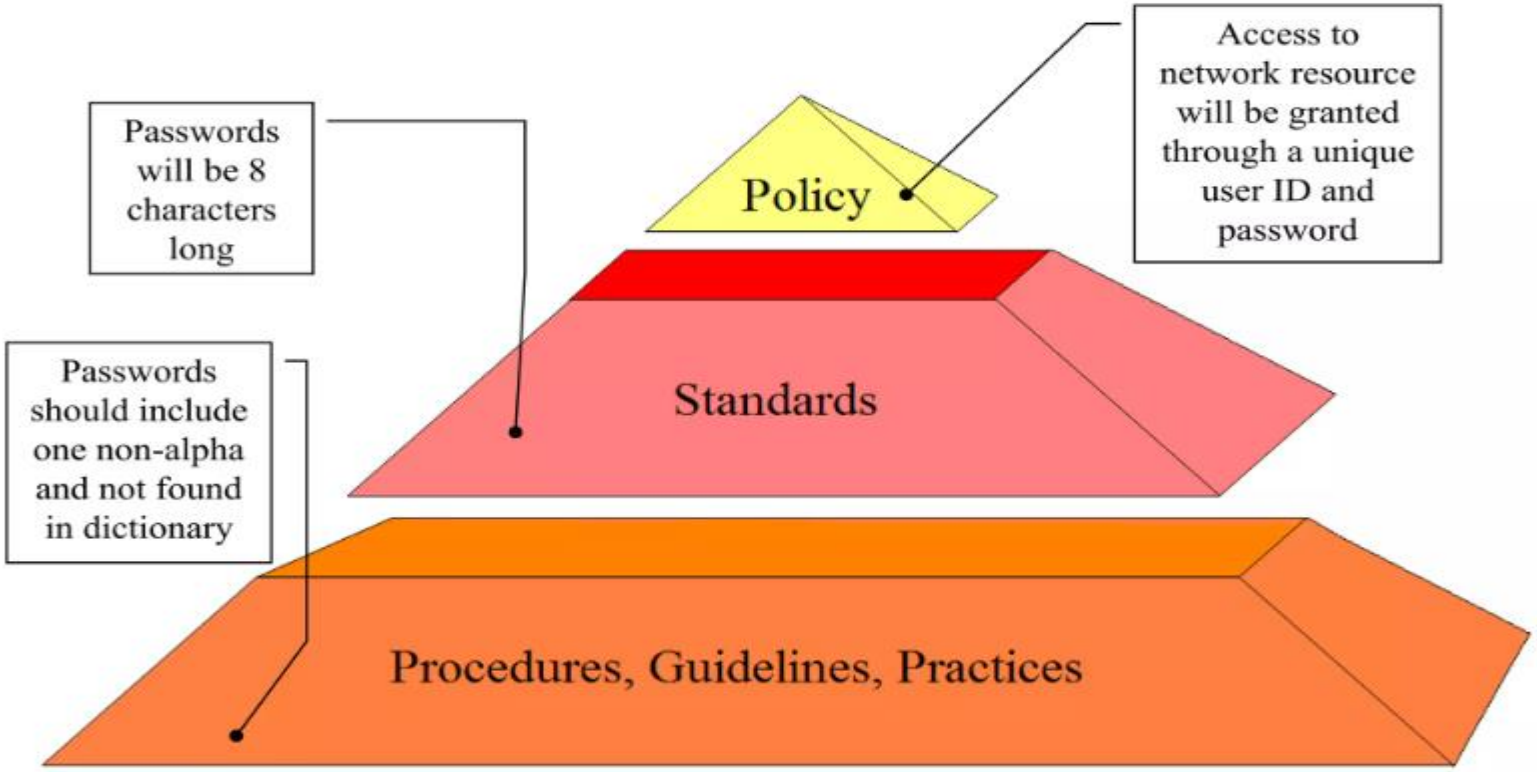
What is Information Security?

- The protection of information and its critical e lements, including systems and hardware that use, store, and transmit that information
- Necessary tools: policy, awareness, training, e ducation, technology
- C.I.A. triangle was standard based on confiden tiality, integrity, and availability
- C.I.A. triangle now expanded into list of critica l characteristics of information

How can information security be achieved?

Information Security is achieved by implementing a suitable set of controls, which could be:

These controls need to be established in order to ensure that the specific security objectives of the organization are met.



What is Risk?

- Risk is the probability that a particular security threat will exploit a particular vulnerability.
- Risk is the likelihood that a loss will occur. Losses occur when a threat exposes a vulnerability. Organizations of all sizes face risks. Some risks are so severe they cause a business to fail.
- Other risks are minor and can be accepted without another thought. Companies use risk management techniques to identify and differentiate severe risks from minor risks. When this is done properly, administrators and managers can intelligently decide what to do about any type of risk.
- The end result is a decision to avoid, transfer, mitigate, or accept a risk

What is Risk?

- Risk management **isn't intended to be risk elimination**. That isn't a reasonable goal. Instead, risk management attempts to identify the risks that **can be minimized and implement controls** to do so.
- Risk management includes several elements:

Business function

- **Business functions** are the activities a business performs to sell products or services.
- **Examples:**
  - **Salespeople regularly** call or email customers. If the capabilities of either phones or email are reduced, sales are reduced.
  - **A Web site sells products** on the Internet. If the Web site is attacked and fails, sales are lost.
  - **Authors write articles** that must be submitted by a deadline to be published. If the author's PC becomes infected with a virus, the deadline passes and the article's value is reduced.

Business Assets

- **A business asset** is anything that has measurable value to a company.
- Assets can have both tangible and intangible values.
  - The tangible value is the actual cost of the asset.
  - The intangible value is value that cannot be measured by cost, such as client confidence.
- Example:
  - Imagine that your company sells products via a Web site. The Web site earns $5,000 an hour in revenue.
  - Now, imagine that the Web server hosting the Web site fails and is down for two hours. The costs to repair it total $1,000. What is the tangible loss?

Business Assets..

- **Example ..**
  - Lost revenue: $5,000 times two hours 5 = $10,000
  - Repair costs: $1,000
  - Total tangible value: $11,000
- The intangible value isn't as easy to calculate but is still very important.
- Imagine that several customers tried to make a purchase when the Web site was down.
  - If the same product is available somewhere else, they probably bought the product elsewhere.
  - That lost revenue is the tangible value.

Business Assets..

- **Intangible value includes:**
  - **Future lost revenue:** Any additional purchases the customers make with the other company is a loss to your company.
  - **Cost of gaining the customer:** A lot of money is invested to attract customers. It is much easier to sell to a repeat customer than it is to acquire a new customer. If you lose a customer, you lose the investment.
  - **Customer influence:** Customers have friends, families, and business partners. They commonly share their experience with others, especially if the experience is exceptionally positive or negative.

Business Assets..

- **Tangible Assets includes:**
  - **Computer systems:** Servers, desktop PCs, and mobile computers are all tangible assets.
  - **Network components:** Routers, switches, firewalls, and any other components necessary to keep the network running are assets.
  - **Software applications:** Any application that can be installed on a computer system is considered a tangible asset.
  - **Data:** This includes the large-scale databases that are integral to many businesses. It also includes the data used and manipulated by each employee or customer.

Profitability versus Survivability

- **Profitability:** The ability of a company to make a profit.
  - Profitability is calculated as revenues minus costs.
- **Survivability:** The ability of a company to survive loss due to a risk.
  - Some losses such as fire can be disastrous and cause the business to fail.

Thank you