Information Security and Network Security

Chapter – 1

Introduction to Information Security

Vulnerabilities and Risks

Vulnerability is the absence or weakness of a safeguard minor threat having the potential to become a greater threat because of vulnerability. It is threat that gets through safeguard into the system.

'vulnerability' is a potential avenue of attack. Vulnerabilities may exist in computer system as well as in the network security data against illegal access and alteration of information during transit in major issue.

As far as OS security in concerned 'vulnerability' is programming error that enables an attacker or virus to gain entry to computer allowing access to confidential information, the running malicious (intended to do harm) program or even crashing the system. vulnerability in also defined as a defect that enables an attacker to by pass security measures once vulnerabilities are reported they are typically patched by the software maker, removing the error unlike the data for general defects in a commercial OS which are usually hard to obtain, the actual data about known vulnerabilities found in major Oss are available for analysis.

Vulnerability Assessment (VA) is often part of the BIA (Business Impact Analysis) process. It is similar to risk analysis/assessment in that there is a quantitative part to estimate the financial damage arising out of a vulnerability and qualitative (operational) part. The extent and scope of vulnerability assessment/analysis is smaller than a full-fledged risk analysis / assessment. VA is to focused solely for the business continuity plan or DR plan.

A function of vulnerability assessment/ analysis is to conduct a loss impact analysis two parts

1. Financial assessment and
2. Operational assessment

Quantitative Loss (criteria)

1. Financial loses owing to negative impact on revenues, capital expenditure or personal liability resolution;
2. Any additional operational expenses in cured owing to the disruptive event (disaster).
3. Financial losses from resolution of violation of contractual agreements.
4. Finial losses from resolution of regulatory or compliance requirements violated.

Critical support areas to be defined during the vulnerability analysis include the following.

1. Tc (Technical Committee), data communications and other IT areas.
2. Physical infrastructure or plant facilities and transportation/logistics services;

3. Accounting, payroll, transaction process (TP), customer sales processing services, Procurement and other allied services.

   On the technical side, there has been the advent and maturation of automated vulnerability scanning tools. When these tools are run appropriately, they help to identify known vulnerabilities in OS; and application systems.

Vulnerability Scanning – in an active scan of system. Using industry standard tools, the auditor may scan network. For known system vulnerabilities. For this, auditor will need both indirect (via the internet) and direct access to network.

Vulnerability to network the automated process of proactively identifying vulnerabilities of computing system in a network in order to determine if and where a system can be exploited (make full use of) and/or threatened. Vulnerability scanning typically refers to the scanning of systems that are connected to the internet. It can also refer to system audits on internal networks that are not connected to the internet in order so access the threat of rogue (unprincipled) software or malicious employees in an enterprise.

While public servers are important for communication and data transfer over the internet they open the door to potential security breaches by the threat agents. Such as malicious hackers. Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing system for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security.

An automated vulnerability scanner will often identity possible vulnerabilities based on services banners or other network responses that may not be what they seem. A vulnerability assessor will stop just before compromising a system, where as a penetration tester will go as far as they can within the scope of the contract.

- **Assess Vulnerability**

  The purpose of assessing vulnerability is to identify and characterize system security vulnerabilities. These vulnerabilities are independent of any particular threat or attack. This set of activities is performed any time during a system's life cycle to support the decision to develop maintain or operate the system within the known environment.

  The goal here is that an understanding of system security vulnerabilities within a defined environment in active base practices:

  1. Select the methods techniques and criteria by which security system vulnerabilities in a defined environment are identified and characterized.
  2. Identify system security vulnerabilities.
  3. Gather data related to the properties of vulnerabilities.
  4. Asses the system vulnerability and aggregate vulnerability that result from specific vulnerabilities and combinations of specific vulnerabilities.
  5. Monitor ongoing changes in the applicable vulnerabilities and change to their characteristics.

Risk Management

Risk can be defined as the possibility of suffering a loss. e.g. the data on the internet of organization in at risk if virtual employees such as the employees on contract can access the data. Therefore, measuring the probability of occurrence of the adverse event enables to estimate the impact of the risk.

How is risk expressed –

Risk is expressed as the probability of the effects associated with a particular activity or activities.

Risk in a function of the following –

- An adverse event
- The probability of the adverse event occurring.

Understanding Risk –

Even day to day life unintentionally or unknowingly pay suffering loss. E.g. we look both ways before crossing the road. Risk in related to uncertainty. The more risk more chance to lose or gain.

How to the measure Risks –

The most basic or expected function of any risk measurement method in determine, as accurately as possible, the risk affects and its impact. A risk measurement method also enables us to determine cost – effective counter measures to control a risk.

Information Risk management –

Today organizations are investing heavily on computer systems and information technology process and methods to gain a competitive edge in the market. Critical business information is being stored, proceed and transferred through the electronic medium.

However, along with the advantages, technology brings various threats to information and network resources. Eavesdropping (secretly listen to conversation), spamming (send the same message indiscriminately to large number of users), tampering (interfere with information in order to damage or make unauthorized alterations), computer viruses and spoofing have become serious issues.

IS (Information System) risk management enables organizations to identify and manage the potential risks associated with information and information technology in cost effective way. IS risk management addresses all the components of information security risk, which are assets, threats, vulnerabilities, risk impacts and countermeasures.

Risk identification –

Before we begin the process of risk management we need to identify what is at risk and what are the risks. This phase is known as risk identification. It is precursor to the risk analysis and assessment phase of the IS risk management process. After we identify the risks we can analyze them to determine their potential impact and likely hood occurrence.

1. Identify Assets - H/w, S/w, Doc data & personnel.
2. Identify the value and impact of assets – value of each of asset.
3. Identify the vulnerabilities associated with an asset.
4. Identify threats faced by an asset – Natural Disaster and Accident.
5. Perform risk Analysis

❖ **IS risk management process –**

The confidentiality, integrity and availability of information have become the need of hour. Organization are eagerly:

- Considering the management of information security risk as an integral part of the risk management process.
- Establishing and implementing and systematic plan for information security risk management.

The is risk management process helps to understand the risks involved in a project and defines methods to manage them. The IS risk management process consists of the following three phases:

1. Risk Analysis and assessment

Before risks can be managed they must be identified. In the risk analysis and assessment phase, identify the factors that can cause a risk. In this phase search and locate risks before they become problems that can adversely affect the project in future.

The identification of risks associated with a project should start when the concept of the project is first developed. The early identification of risks enables organizations to quickly mitigate (make less sever serious or painful) these risks before they have any significant effect.

Common risk can be identified from the past experience of the project team and from the documents of earlier projects. The most common way to identify risks are:

- Establish an environment that constantly encourages employees to raise concerns and issues.
- Conduct quality reviews spanning (extend period of time) the development cycle of a project.
- After identifying risk, review the risk to determine its cause possibility and expected consequence in terms of its financial impacts. It is also necessary to prioritize risk according to their severity level.

The risk analysis and assessment phase require high levels of participation from the people associated with the project.

2. Risk planning and Implementation

After analyzing risks, we create cost- effective action plans to manage risks. After designing cost- effective plans, your impalement the actions decided for protecting the assets.

In this phase the result of risk analysis is documented and reviewed by the project sponsor management committee. The documents include:

- The description of risk.

- The probable cause of the risk.
- The possibility that the risk will occur.
- The impact of risk

3. Risk mitigation (make less server and monitoring)

In this phase ensure that actions are taken to mitigate the existing risks. At times, previously identified risk changes during the course of development. This is either due to internal pressure, such as revised business requirements or external pressure, such as legislation changes. Therefore, extreme care must be taken to ensure that project management attention in not only focused on previously identified risks but also on the possibility of new risks.

Human Behavioral Risks

A person can play as variety of roles such as the user of information systems, owner of information systems and hacker or attacker as IS. Several studies have implicated people as weak link in the information security chain. Sharing username, password with their colleagues writing them down the desk or monitor, opening unknown emails and their attachments, downloading S/W from the internet, leaving systems in login status while unattended are examples of human mistake in the domain of information security. Indeed, users intentionally or unintentionally are a great potential threat to information assets. In this dynamic environment effective information security knowledge sharing among employees not only increase the level of awareness as an effective approach, but also reduces the cost of information security in the organizations.

The motivation for knowledge sharing among employees is the important challenge in this realm (field). Sharing previous relevant experiments in the domain of information security is a valuable resource in information security awareness.

Social Engineering

Social Engineering is the practice of misleading a person to obtain important information. In this manner, a social engineer in able to receive the required information without raising any suspicion.

Some vulnerabilities that aid the threat from social engineering are:

- Lack of policies that restrict employees to provide information over phone.
- Lack of policies that require all customer calls to be withheld until the identity of the customer is verified.