Scan or click here for more resources


**Antivirus:** It prevent the installation of the virus, scan the system for virus that are already install.

**Types of Application Security:**

- **Authentication:** Authentication is a method of ensuring that only authorized users. A weakness known as cross-site scripting (XSS) permits an attacker to introduce client-side code into a site page. The attacker gets direct access to the user's data.rs to have access of controlling the application. Authentication methods confirm that the user is who they guarantee to be. While signing into an application, this can be performed by requiring the user to supply a user name and password. There is also multi-level authentication which ensures maximum security, for example, something you know (a password), something you have(a cell phone), and something you are (a biometric).
- **Authorization:** After authentication, the user is allowed to access and use the application. The application of the user is only validated after comparing the identification of the user to approve the access, thus authentication has to be always before the authorization step.
- **Encryption:** After the verification and authorization of the user while using the application other security protocols can protect the data from threats. Encryption is done to keep sensitive data safe while flowing from end-user to cloud in cloud-based applications.
- **Logging:** Assuming a security break happens in an application, logging can help with figuring out who accessed the data and how it happened. Application log records monitor who accessed and what portions of the application have been accessed.
- **Application Security Testing:** A strategy that guarantees that these security controls are working actually.

# Data Security Consideration

Data security is the protection of programs and data in computers and communication systems against unauthorized access, modification, destruction, disclosure or transfer whether accidental or intentional by building physical arrangements and software checks. It refers to the right of individuals or organizations to deny or restrict the collection and use of information about unauthorized access. Data security requires system managers to reduce unauthorized access to the systems by building physical arrangements and software checks.

Data security uses various methods to make sure that the data is correct, original, kept confidentially and is safe. It includes-

- Ensuring the integrity of data.
- Ensuring the privacy of the data.
- Prevent the loss or destruction of data.

Data security consideration involves the protection of data against unauthorized access, modification, destruction, loss, disclosure or transfer whether accidental or intentional. Some of the important data security consideration are described below:

## Backups

**Data backup refers to save additional copies of our data in separate physical or cloud locations from data files in storage. It is essential for us to keep secure, store, and backup our data on a regular basis. Securing of the data will help us to prevent from-**

- Accidental or malicious damage/modification to data.
- Theft of valuable information.
- Breach of confidentiality agreements and privacy laws.
- Premature release of data which can avoid intellectual properties claims.
- Release before data have been checked for authenticity and accuracy.

Keeping reliable and regular backups of our data protects against the risk of damage or loss due to power failure, hardware failure, software or media faults, viruses or hacking, or even human errors.

To use the Backup 3-2-1 Rule is very popular. This rule includes:

- Three copies of our data
- Two different formats, i.e., hard drive+tape backup or DVD (short term)+flash drive
- One off-site backup, i.e., have two physical backups and one in the cloud

**Some important backup options are as follows-**

1. Hard drives - personal or work computer
2. Departmental or institution server

3. External hard drives
4. Tape backups
5. Discipline-specific repositories
6. University Archives
7. Cloud storage

Some of the top considerations for implementing secure backup and recovery are-

1. Authentication of the users and backup clients to the backup server.
2. Role-based access control lists for all backup and recovery operations.
3. Data encryption options for both transmission and the storage.
4. Flexibility in choosing encryption and authentication algorithms.
5. Backup of a remote client to the centralized location behind firewalls.
6. Backup and recovery of a client running Security-Enhanced Linux (SELinux).
7. Using best practices to write secure software.

## Archival Storage

Data archiving is the process of retaining or keeping of data at a secure place for long-term storage. The data might be stored in safe locations so that it can be used whenever it is required. The archive data is still essential to the organization and may be needed for future reference. Also, data archives are indexed and have search capabilities so that the files and parts of files can be easily located and retrieved. The Data archival serve as a way of reducing primary storage consumption of data and its related costs.

Data archival is different from data backup in the sense that data backups created copies of data and used as a data recovery mechanism to restore data in the event when it is corrupted or destroyed. On the other hand, data archives protect the older information that is not needed in day to day operations but may have to be accessed occasionally.

Data archives may have many different forms. It can be stored as Online, offline, or cloud storage-

- Online data storage places archive data onto disk systems where it is readily accessible.
- Offline data storage places archive data onto the tape or other removable media using data archiving software. Because tape can be removed and consumes less power than disk systems.
- Cloud storage is also another possible archive target. For example, Amazon Glacier is designed for data archiving. Cloud storage is inexpensive, but its costs can grow over time as more data is added to the cloud archive.

The following list of considerations will help us to improve the long-term usefulness of our archives:

1. Storage medium
2. Storage device
3. Revisiting old archives
4. Data usability
5. Selective archiving
6. Space considerations
7. Online vs. offline storage

## Disposal of Data

Data destruction or disposal of data is the method of destroying data which is stored on tapes, hard disks and other electronic media so that it is completely unreadable, unusable and inaccessible for unauthorized purposes. It also ensures that the organization retains records of data for as long as they are needed. When it is no longer required, appropriately destroys them or disposes of that data in some other way, for example, by transfer to an archives service.

The managed process of data disposal has some essential benefits-

- It avoids the unnecessary storage costs incurred by using office or server space in maintaining records which is no longer needed by the organization.
- Finding and retrieving information is easier and quicker because there is less to search.

The disposal of data usually takes place as part of the normal records management process. There are two essential circumstances in which the destruction of data need to be handled as an addition to this process-

- The quantity of a legacy record requires attention.
- The functions are being transferred to another authority and disposal of data records becomes part of the change process.

The following list of considerations will help us for the secure disposal of data-

1. Eliminate access
2. Destroy the data
3. Destroy the device
4. Keep the record of which systems have been decommissioned
5. Keep careful records
6. Eliminate potential clues
7. Keep systems secure until disposal

## Threat to E-Commerce

E-Commerce refers to the activity of buying and selling things over the internet. Simply, it refers to the commercial transactions which are conducted online. E-commerce can be drawn on many technologies such as mobile commerce, Internet marketing, online transaction processing, electronic funds transfer, supply chain management, electronic data interchange (EDI), inventory management systems, and automated data collection systems.

E-commerce threat is occurring by using the internet for unfair means with the intention of stealing, fraud and security breach. There are various types of e-commerce threats. Some are accidental, some are purposeful, and some of them are due to human error. The most common security threats are an electronic payments system, e-cash, data misuse, credit/debit card frauds, etc.

## Electronic payments system:

With the rapid development of the computer, mobile, and network technology, e-commerce has become a routine part of human life. In e-commerce, the customer can order products at home and save time for doing other things. There is no need of visiting a store or a shop. The customer can select different stores on the Internet in a very short time and compare the products with different characteristics such as price, colour, and quality.

The electronic payment systems have a very important role in e-commerce. E-commerce organizations use electronic payment systems that refer to paperless monetary transactions. It revolutionized the business processing by reducing paperwork, transaction costs, and labour cost. E-commerce processing is user-friendly and less time consuming than manual processing. Electronic commerce helps a business organization expand its market reach expansion. There is a certain risk with the electronic payments system.

### E-cash

E-cash is a paperless cash system which facilitates the transfer of funds anonymously. E-cash is free to the user while the sellers have paid a fee for this. The e-cash fund can be either stored on a card itself or in an account which is associated with the card. The most common examples of e-cash system are transit card, PayPal, GooglePay, Paytm, etc.

E-cash has four major components-

1. **Issuers** - They can be banks or a non-bank institution.
2. **Customers** - They are the users who spend the e-cash.
3. **Merchants or Traders** - They are the vendors who receive e-cash.
4. **Regulators** - They are related to authorities or state tax agencies.

In e-cash, we stored financial information on the computer, electronic device or on the internet which is vulnerable to the hackers. Some of the major threats related to e-cash system are-


E-cash Threats

## Backdoors Attacks

It is a type of attacks which gives an attacker to unauthorized access to a system by bypasses the normal authentication mechanisms. It works in the background and hides itself from the user that makes it difficult to detect and remove.

## Denial of service attacks

A denial-of-service attack (DoS attack) is a security attack in which the attacker takes action that prevents the legitimate (correct) users from accessing the electronic devices. It makes a network resource unavailable to its intended users by temporarily disrupting services of a host connected to the Internet.

## Direct Access Attacks

Direct access attack is an attack in which an intruder gains physical access to the computer to perform an unauthorized activity and installing various types of software to compromise security. These types of software loaded with worms and download a huge amount of sensitive data from the target victims.

## Eavesdropping

This is an unauthorized way of listening to private communication over the network. It does not interfere with the normal operations of the targeting system so that the sender and the recipient of the messages are not aware that their conversation is tracking.

## Credit/Debit card fraud

A credit card allows us to borrow money from a recipient bank to make purchases. The issuer of the credit card has the condition that the cardholder will pay back the borrowed money with an additional agreed-upon charge.

A debit card is of a plastic card which issued by the financial organization to account holder who has a savings deposit account that can be used instead of cash to make purchases. The debit card can be used only when the fund is available in the account.

# Cyber Security Risk Analysis

Risk analysis refers to the review of risks associated with the particular action or event. The risk analysis is applied to information technology, projects, security issues and any other event where risks may be analysed based on a quantitative and qualitative basis. Risks are part of every IT project and business organizations. The analysis of risk should be occurred on a regular basis and be updated to identify new potential threats. The strategic risk analysis helps to minimize the future risk probability and damage.

**Enterprise and organization used risk analysis:**

- To anticipates and reduce the effect of harmful results occurred from adverse events.
- To plan for technology or equipment failure or loss from adverse events, both natural and human-caused.
- To evaluate whether the potential risks of a project are balanced in the decision process when evaluating to move forward with the project.
- To identify the impact of and prepare for changes in the enterprise environment.

# Types of Risk Analysis

The essential number of distinct approaches related to risk analysis are:

## Qualitative Risk Analysis

- The qualitative risk analysis process is a project management technique that prioritizes risk on the project by assigning the probability and impact number. Probability is something a risk event will occur whereas impact is the significance of the consequences of a risk event.
- The objective of qualitative risk analysis is to assess and evaluate the characteristics of individually identified risk and then prioritize them based on the agreed-upon characteristics.
- The assessing individual risk evaluates the probability that each risk will occur and effect on the project objectives. The categorizing risks will help in filtering them out.
- Qualitative analysis is used to determine the risk exposure of the project by multiplying the probability and impact.

## Quantitative Risk Analysis

- The objectives of performing quantitative risk analysis process provide a numerical estimate of the overall effect of risk on the project objectives.
- It is used to evaluate the likelihood of success in achieving the project objectives and to estimate contingency reserve, usually applicable for time and cost.
- Quantitative analysis is not mandatory, especially for smaller projects. Quantitative risk analysis helps in calculating estimates of overall project risk which is the main focus.