

Chapter-#09


Data Security Consideration

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.

Data Security Consideration

- Some of the important data security consideration are described below:



The diagram consists of a large, light-orange rounded rectangle containing three smaller, horizontally-oriented rectangles stacked vertically. The top rectangle is yellow and labeled 'Backups'. The middle rectangle is purple and labeled 'Archival Storage'. The bottom rectangle is green and labeled 'Disposal Of Data'. The entire diagram is set against a background of green geometric shapes on the right side of the slide.

Backups

Archival Storage

Disposal Of Data

Data Security Consideration

Data Security Consideration

► 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.

Data Security Consideration

- ▶ 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-
- ▶ Hard drives - personal or work computer
- ▶ Departmental or institution server
- ▶ External hard drives
- ▶ Tape backups
- ▶ Discipline-specific repositories
- ▶ University Archives
- ▶ Cloud storage

Data Security Consideration

- ▶ **Some of the top considerations for implementing secure backup and recovery are-**
- ▶ Authentication of the users and backup clients to the backup server.
- ▶ Role-based access control lists for all backup and recovery operations.
- ▶ Data encryption options for both transmission and the storage.
- ▶ Flexibility in choosing encryption and authentication algorithms.
- ▶ Backup of a remote client to the centralized location behind firewalls.
- ▶ Backup and recovery of a client running Security-Enhanced Linux (SELinux).
- ▶ Using best practices to write secure software.

Data Security Consideration

► 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 Security Consideration

- ▶ 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.

Data Security Consideration

- ▶ The following list of considerations will help us to improve the long-term usefulness of our archives:
- ▶ Storage medium
- ▶ Storage device
- ▶ Revisiting old archives
- ▶ Data usability
- ▶ Selective archiving
- ▶ Space considerations
- ▶ Online vs. offline storage

Data Security Consideration

► Storage medium

► The first thing is to what storage medium we use for archives. The archived data will be stored for long periods of time, so we must need to choose the type of media that will be lost as long as our retention policy dictates.

► Storage device

► This consideration takes into account about the storage device we are using for our archives which will be accessible in a few years. There is no way to predict which types of storage devices will stand the best. So, it is essential to try to pick those devices that have the best chance of being supported over the long term.

Data Security Consideration

- ▶ **Revisiting old archives**
- ▶ Since we know our archive policies and the storage mechanisms we use for archiving data would change over time. So we have to review our archived data at least once a year to see that if anything needs to be migrated into a different storage medium.
- ▶ **For example,**
- ▶ about ten years ago, we used Zip drives for archival then we had transferred all of my archives to CD. But in today's, we store most of our archives on DVD. Since modern DVD drives can also read CDs, so we haven't needed to move our extremely old archives off CD onto DVD.

Data Security Consideration

► Data usability

► In this consideration, we have seen one major problem in the real world is archived data which is in an obsolete format.

► For example,

► a few years ago, document files that had been archived in the early 1990s were created by an application known as PFS Write. The PFS Write file format was supported in the late 80s and early 90s, but today, there are not any applications that can read that files. To avoid this situation, it might be helpful to archive not only the data but also copies the installation media for the applications that created the data.

► Selective archiving

► In this consideration, we have to sure about what should be archived. That means we will archive only a selective part of data because not all data is equally important.

Data Security Consideration

► Space considerations

► If our archives become huge, we must plan for the long-term retention of all our data. If we are archiving our data to removable media, capacity planning might be simple which makes sure that there is a free space in the vault to hold all of those tapes, and it makes sure that there is a room in our IT budget to continue purchasing tapes.

► Online vs. offline storage

► In this consideration, we have to decide whether to store our archives online (on a dedicated archive server) or offline (on removable media). Both methods of archival contain advantages and disadvantages. Storing of data online keeps the data easily accessible. But keeping data online may be vulnerable to theft, tampering, corruption, etc. Offline storage enables us to store an unlimited amount of data, but it is not readily accessible.

Data Security Consideration

► 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.

Data Security Consideration

- ▶ 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-
- ▶ Eliminate access
- ▶ Destroy the data
- ▶ Destroy the device
- ▶ Keep the record of which systems have been decommissioned
- ▶ Keep careful records
- ▶ Eliminate potential clues
- ▶ Keep systems secure until disposal

Data Security Consideration

► Eliminate access

► In this consideration, we have to ensure that eliminating access account does not have any rights to re access the disposed of data again.

► Destroy the Data

► In this consideration, there is not necessary to remove data from storage media will be safe. Even these days reformatting or repartitioning a drive to "erase" the data that it stores is not good enough. Today's many tools available which can help us to delete files more securely. To encrypt the data on the drive before performing any deletion can help us to make data more difficult to recover later.

Data Security Consideration

► Destroy the device

► In the most cases, storage media need to be physically destroyed to ensure that our sensitive data is not leaked to whoever gets the drives next. In such cases, we should not destroy them itself. To do this, there should be experts who can make probably a lot better at safely and effectively rendering any data on our drives unrecoverable. If we can't trust this to an outsider agency that specializes in the secure destruction of storage devices, we should have a specialized team within our organization who has the same equipment and skills as outside contractors.

► Keep the record of which systems have been decommissioned

► In this, we have to make sure that the storage media has been fully decommissioned securely and they do not consist of something easily misplaced or overlooked. It is best if storage media that have not been fully decommissioned are kept in a specific location, while decommissioned equipment placed somewhere else so that it will help us to avoid making mistakes.

Data Security Consideration

► Keep careful records

- In this consideration, it is necessary to keep the record of whoever is responsible for decommissioning a storage media. If more than one person is assigned for such responsibility, he should sign off after the completion of the decommissioning process. So that, if something happened wrong, we know who to talk to find out what happened and how bad the mistake is.

► Eliminate potential clues

- In this consideration, we have to clear the configuration settings from networking equipment. We do this because it can provide crucial clues to a security cracker to break into our network and the systems that reside on it.

► Keep system secure until disposal of data

- In this consideration, we should have to make clear guidelines for who should have access to the equipment in need of secure disposal. It will be better to ensure that nobody should have access authentication to it before disposal of data won't get his or her hands on it.