Journal of Policy Research, 7(4), 50-53.
https://jprpk.com

From Data Backup to Data Restoration: A Research Strategy and Policy

Waleed Younus[1*]

Abstract:
In an increasingly digital business environment, backing up data is essential for an organization. An unsafe computer program can ruin your hard-earned information. In today's digital landscape, where data plays a crucial role in the success and continuity of businesses and organizations, ensuring its safety and availability is of paramount importance. Data backup and restoration are essential components of any robust IT strategy, as they provide safeguards against data loss, system failures, natural disasters, or malicious attacks. Backup is a practice that combines strategies and solutions to make a backup effective and inexpensive. Data is copied to one or more locations, with pre-determined frequencies, and with varying intensity. Set up a flexible backup job, use your architecture, or use available backup solutions as a (BaaS) backup, and mix them with local storage. Data restoration, on the other hand, involves a set of policies, tools, and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster. It focuses on restoring IT operations critical to the resumption of business. Policies are high-level statements that are equal to organizational scope and drive the decision-making process within the organization. In this research paper, we explain different aspects of Data Backup and Restoration in organizations. This practice ensures that in the event of hardware failure, accidental deletion, or mishandling, data backup and restoration policy guide in quick resume of essential data for normal operations.

Keywords: Data, Data collection, Data backup, Data Restoration, Hospital Management Information System (HMIS), Information Technology (IT), Management Information System (MIS), Data Base Administrator (DBA)

1. Introduction

Data has always been and is becoming a resource that needs to be judiciously used and shared for the benefit of organizations and institutions. More than ever, there is massive data sharing these days with the increasing technological updates and social networking sites. The processed data is called information, and the task of finding it from the existing repository is called information retrieval. [1-5]. Data structures are the different techniques used to store the data in the persistent memory. The purpose of the data structures varies in each application. In [3], the authors classify the data structures based on the purpose for which it is used. The data structures like arrays, linked structures, hash tables are primarily used for storing the data and hence are classified as storage structures. The other category of data structures such as stacks, queues and priority queues are used for processing the data and these are classified as process-oriented data structures. There are still some data structures left out, which not only simply store the data but yield to the description of the data by the way it is arranged in it. Collections, sets, linear lists, binary trees, etc. are the data structures which describe the nature of the data held in it and hence the authors call it descriptive data structures [1-7]

Data collection and storage technology has made it possible for organizations to accumulate huge amounts of data at lower cost. An information security policy is a document designed to ensure the protection of information assets and the secure handling of technological information through specific procedures that support the organization's objectives. [8]. Information security policy ensures information asset and information technology secure with a specific procedure to support an organization aim and goal. an important issue is management support during implementation of information security policies. When support is obtained, another challenge faced is ensuring that policies are truly able to improve security [9]. Management can be compared to technical products in terms of efficiency, but achieving efficient value policies is often more challenging. This is easier for technical products because their efficiency can often be debated based on statistics. Even when an organization implements security policies, it is often found that employees ignore rules and exhibit unexpected behavior. Without compliance, policies remain only as words on paper or bits in which they are stored. Compliance with policies aims to ensure the application of organizational security standards. [10]. Previous researchers have investigated to formulate the model of user compliance with information security policies. Bulgurcu (2010) investigates rationality-based factors that encourage an employee to comply with ISP requirements concerning protecting information resources and organizational technology and argue that employee attitudes are influencing by compliance benefits, compliance costs, and non-compliance costs, which are beliefs about valuation as consequences of compliance or non-compliance [11]. Users often overlook the importance of adhering to security policies until incidents occur, leading to significant impacts on organizations, which then face additional costs due to non-compliance. As the volume of data continues to grow, the

[1] Fauji Foundation Head Office, 68-Tipu Road, Chakala Cantt, Rawalpindi, Pakistan
*Corresponding Author, Email Address: waleed.younus@gmail.com

necessity for efficient data retrieval becomes more pronounced. In response to this need, a system known as "information retrieval systems" was introduced, designed to facilitate the effective retrieval of stored data." (IRS) [12].

2. Data Backup and Restoration Policy and Strategy

This document provides the Proposed Strategy for Backup / Recovery of HMIS Application

2.1 Purpose

The purpose of the Data Backup Plan is to establish and implement procedures to create and maintain retrievable exact copies of the whole database items and related technology components that are necessary for recovery activities. This document will define the following standards for organization backup processing.

3. Policy Statement

1. IT/MIS Manager is responsible for backing up IT-managed servers and must implement a tested and auditable process to facilitate recovery from data loss.
2. All departments should store data on network storage (e.g., T drive, OneDrive) rather than local storage (e.g., Windows or Mac hard drive). Local storage is not backed up by IT servers and will be the responsibility of the Information Owner to protect the data with adequate backups.
3. Network Administrator will perform daily data backups of all Information Technology managed servers containing critical data for the purposes listed above.
   - Individual drives (e.g., S drive, profile) and email will be retained for 14 days.
   - All other data, such as Enterprise Application Data (e.g., Banner and Oracle data) and shared storage backups (e.g., T drive, Files) will be retained for 60 days.
   - Policy exceptions to the stated retention times will be at the discretion of the President utilizing the Information Technology Policy Exception Form.
4. Data identified by the Information Owner as non-critical may be excluded from this policy.
5. Alternative backup schedules and media management may be requested by the Information Owner commensurate with the criticality of the data and the capabilities of the tools used for data storage.
6. Records retention is the responsibility of the Information Owner. The Information Technology backups are not to be used to satisfy the retention of records and are not customized for all the varying retention periods.
7. Data Backup will be stored at a location that is physically different from the original location.
8. Verification, through restoration of backed-up data, must be performed on Monthly basis and perform dry run on Training server as defined by the Information Technology back-up procedures document for the respective system.
9. Procedures for backing up of critical data and the testing of the procedures must be documented. Such procedures must include at a minimum for each type of data:
   - A definition of the specific data to be backed up.
   - The backup method to be used (full backup, incremental backup, differential, mirror, or a combination).
   - The number of generations of backed up data that are to be maintained (both on site and off site).
   - The responsible individual(s) for data backup.
   - The storage site(s) for the backups.
   - The storage media to be used.
   - The naming convention for the labels on storage media.
   - Any requirements concerning the data backup archives.
   - The data transport modes.
   - For data transferred during any backup process, end-to-end security of the transmission path must be ensured for confidential data.
   - The recovery of backed up data.
   - Processes must be maintained, reviewed, and updated periodically to account for new technology, business changes, and migration of applications to alternative platforms.

4. Types of Backup / Recovery for Database

- Point in Time
- Full Cold Backup
- Logical Backups
- Schema / User level
- Incremental
- Ad hoc backups when requested or deemed necessary by DBA

4.1. Operational Backup Standard

4.1.1 Daily backups

A Level 1 dump is written to a file which is stored on the local hard disk (or directly on external drive) of the backup server. Once the backup process completed the backup files copied on the external drive then moved to remote location as an off sight backup.

4.1.2 Weekly backups

Once a week (on Sunday) a full backup is written on the local hard disk (or directly on external drive) and then moved to remote location as an off sight backup.

4.1.3 Monthly backups

Once a month, the entire database is backed up onto its own tape (the tap set that dedicated for monthly backup) with the RMAN backup utility. This is a full backup, also known as a level 0 dump.

4.2 Hardware & Media Recommendation

4.2.1 Test or Training server

To comply with this backup policy a dedicated Training server is required. Currently this requirement is already met by all hospitals where HMIS system is running. This training server will be used for

- Testing of Application Backup
- Training of end user(s).

4.2.2 Removable Device

Following are some of the recommendations as per hospital regarding Removable Device(s).

Sr.No	Hospital Name	No. of Device	Device Specification
1	Hospital Lahore	01	04 Terabyte
2	Hospital Peshawar	01	02 Terabyte
3	Hospital Karachi	01	02 Terabyte
4	Hospital Kallar Kahar	01	02 Terabyte
5	Hospital Jhelum	01	02 Terabyte
6	Hospital Lahore	01	02 Terabyte

4.3 Software

Although there is various software available in the market to get a secure database backup but the most suitable and highly recommended tool is the Oracle RMAN which comes along with the Oracle software. It provides very efficient and quick ways to get restoration of data in case of any disaster/crash of database server.

4.4 Retention

Full backups [DB Dump with Application] retained for a period of 7 days. The backup scripts automatically delete the obsolete backup sets.

4.5 Verification

Oracle RMAN utility provides the backup verification features. Within the backup script the backup verification commands are also embedded to verify the current backup and in case of any corruption/error of backup, the current log file will be updated immediately.

4.6 Restoration

In case of any crash/disaster of database server immediate restores are available to users by running the recovery scripts (with the help of DBA). This current backup/ recovery policy guarantees the complete recovery of data.

Backup documentation must be maintained, reviewed and updated periodically to account for new technology, business changes, and migration of applications to alternative platforms. This includes, but is not limited to:

a. Identification of critical data and programs;
b. Documentation and support items necessary to perform essential tasks during a recovery process.

4.6.1 Documentation of the restoration process must include:

a. Procedures for the recovery
b. Provision for key management should the data be encrypted.

4.6.2 Recovery procedures must be tested at least monthly.

4.6.3 Recovery tests must be documented and reviewed by the IT/MIS Manager.

4.7 Location

It is recommended for all MIS Manager(s) to keep Application Backup and DB Dump backup on External Drive and place External drive outside IT data center building.

5. Recommendations

1. It is highly recommended to keep two backups

   a. External drive backup, which should be placed outside IT data center building.
   b. Local hard disk, which can be placed in IT premises
2. MIS Managers of said hospital(s) will be responsible to send the updated Backup [DB Dump & Application] to HMIS Department on quarterly bases.

6. Training Server Update

- It is highly recommended for all MIS Manager(s) to copy Live application and Database on Training server every 02 Months. (BACKUP Drives should be used for copy).
- Necessary scripts will be provided to MIS Manager by HMIS DBA for updating Training Server.

7. Conclusion

The adoption of a policy for data backup and restoration offers significant advantages for organizations. By leveraging data backup and restoration, organizations can improve data availability, reduce recovery time, enhance cost efficiency, and achieve scalability and flexibility. These processes streamline the management of backup and restoration, reducing the need for extensive IT resources. They also enable easier and more frequent testing and validation of backup and restoration plans, ensuring effectiveness when needed. Providers often offer data storage across multiple geographic locations, ensuring data can be restored even if one location is compromised. Additionally, these providers continuously update their services with the latest technologies and best practices, enhancing the resilience of data protection capabilities.

References

[1] S. Ceri et al., Web Information Retrieval, Data-Centric Systems and Applications, DOI 10.1007/978-3-642-39314-3_2, © SpringerVerlag Berlin Heidelberg 201

[2] Falley. P "Categories of Data Structures", Journal of Computing Sciences in Colleges - Papers of the Fourteenth Annual CCSC Midwestern Conference and Papers of the Sixteenth Annual CCSC Rocky Mountain Conference. Volume 23 Issue 1, October 2007. PP. 147-153, 2007-10-01

[3] Fei Song, W Bruce Croft. A general language model for information retrieval. Proceedings of the eighth international conference on Information and knowledge management (ACM) 1999/11/1. pp316-321

[4] B. Zhou and Y. Yao Evaluating information retrieval system performance based on user preference JIIS, 34:227–248, 2010

[5] Nicholajs. B Elkin, W.B Rucec Roft,. Retrieval Techniques, Annual Review of Information Science and Technology, Volume 22. 1987. Martha E. Williams, Editor Published for the American Society for Information Science (ASIS) bv Elsevier Science Publishers.

[6]. V R, Kanagavalli & Maheeja, G. (2016). A Study on the usage of Data Structures in Information Retrieval

[7]. Jain, Nikita. (2013). Data mining techniques: A survey paper. International Journal of Research in Engineering and Technology. 02. 116-119. 10.15623/ijret.2013.0211019.

[8] Doherty, N.F., and H. Fulford H. (2006) "Aligning The Information Security Policy with The Strategic Information Systems Plan." Comput Secur 25: 55–63. doi: 10.1016/j.cose.2005.09.009.

[9] Nohlberg, M. (2009) "Why Humans are the Weakest Link." Soc. Hum. Elem. Inf. Secur. Emerg. Trends. p. 22.

[10] Barry, L. (2013) Information Security Policy Development for Compliance, Boca Raton, CRC Press Taylor & Francis Group.

[11] Bulgurcu, B., H. Cavusoglu, and I. Benbasat. (2010) "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness." MIS Q 34: 523–48. doi:10.1093/bja/aeq366.

[12]. Parul Kalra Bhatia, Tanya Mathur, Tanaya Gupta. Survey Paper on Information Retrieval Algorithms and Personalized Information Retrieval Concept. International Journal of Computer Applications. 66, 6 (March 2013), 14-18. DOI=10.5120/11088-6039