INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN: 2278 – 0211 (Online) / 2278-7631 (Print)

A Study On Data Backup And Recovery Procedure At A Cooperate Hospital

Syed Murtuza Hussain Bakshi
Vice Principal and Associate Professor
Department of hospital management,
Owaisi Hospital and Research Center,
Hyderabad,India

Shaista amreen
OT Manager
Owaisi Hospital and Research Center,
Hyderabad, India

Abstract:

Computer users all across the world are familiar with the problem of lost data such incidents may result in lost work or the deletion of unnecessary files or even loss of important business data that has significance and cost associated with it. Information is an asset like other important business assets which is essential to an organization and consequently needs to be suitably protected especially in interconnected business environment where information is exposed to a growing number and a wider variety of intimidation and vulnerabilities. Management should provide a means to backup relevant data on a regular basis. There are key backup issues that have to be concerned by the management they are media of backup, the reliability of backup process, where the backup is stored and testing the procedure for restoring the backup at least once a year. The study was conducted at 14 tertiary care hospitals with an aim to study various hospital information systems, regular data backup and recovery practices & procedures, comprehend the hardware and network layout. Data is analyzed through Logical and Metaphorical Analysis. It was found out in the study that the backup methods that are followed at the tertiary care hospitals are Incremental Backup and Full Backup with a standard hardware support.

Keywords: *Computers, Data backup and recovery, Hospital Information Systems.*

Introduction

All computer users are familiar with the problem of lost data. Fortunately, most such incidents are relatively inconsequential, representing only a few minutes of lost work or the deletion of unnecessary files. However, sometimes the nature of the lost data is critical and the cost of lost data is significant. As reliance on information and data as economic drivers for businesses continues to increase, owners and managers are subject to new risks (Jon Toiga, 1989).It is important to recognize all business are information driven which include Product data, employee data, partner data, supplier data, financial data, marketing data and more provide the foundation for business transactions and relationships for companies around the world. Information technology in turn has become a critical vehicle for creating, managing and sharing information in organizations of all sizes and in virtually all industries. Together data, information and information systems serve as business enablers in today's highly connected world (Philip L.Wandrei, 2007).

Information is an asset like other important business assets which is essential to an organization's business and consequently needs to be suitably protected. This is especially important in the increasingly interconnected business environment. As a result of this increasing inter connectivity, information is now exposed to a growing number and a wider variety of intimidation and vulnerabilities (Mugoh Leon et al, 2011). As data and information is irreplaceable strategic asset loss or destruction of data can have horrific financial consequences for an organization (Coombs, F. 2008).The protection of data and information is important for the survival of any organization. However, in healthcare it's not just important it is vital. Healthcare is quite different from other sectors, as such backup and disaster recovery needs to be well thought-out in a serious way (Bridgehead software report, 2008).

Management should support and provide a means to backup relevant data on a regular basis. That backup could be to media (e.g., tape or external hard drive), or it could be in a remote location via the cloud (i.e., the Internet). If an enterprise is backed up to the media, the aforementioned principle recommends that backups be conducted to a different medium for end-of-week and end-of-month backups (this daily, weekly and monthly set of backups is known as "grandfather-father-son").The next concern is whether the backup process is reliable. Therefore, upon using a new backup methodology or technology, management should provide a means to test the data afterward to ensure that the process is actually recording all of the data onto the target

backup device. Another concern is where the backup is stored. If it is stored onsite and if the entity suffers a pandemic event such as a fire, the event would destroy the operational data and the backup data. Thus, the backup principle for storage is to provide a location that is at a safe distance from the entity's location. The cloud automatically provides this element. Additionally, management should provide a test for restoring the backup at least once a year. That test should be documented, even if it is just a screenshot showing the data restored (Tommie W. Singleton (2011).

Methods

The study was conducted at 14 tertiary care hospitals which are scattered across India in cities of Hyderabad, Vizag, Pune, Raipur, Bhuwaneshwar, Nagpur and Rajam. All the 14 hospitals are part of the convenient sampling research plan. The present study is Exploratory in nature it is conducted to identify the various hospital information systems that are implemented and to understand the data backup and recovery practices & procedures followed, the hardware and network layout.The data is largely descriptive and categorized as a non-experimental qualitative study .The data is collected through observation & interviews. Extensive interviews were carried out with the individuals who are directly involved with the application system that include 14 information technology managers, 14 database administrators and 2 backup and recovery system managers. Data is analyzed through logical Analysis and Metaphorical Analysis which is in the form of diagrams, pictorial representation with written descriptions and on various metaphors that fit what is observed.

Discussions

The study was carried out at 14 tertiary care hospitals which are scattered across India

The Hospital Information System used across 14 tertiary care hospitals is Jeeva Software provided by the vendor Karishma software solution, now called as Napier. Jeeva provides entire spectrum of solutions, streamline, automate , optimize clinical, administrative and supply-chain functions of the hospital

The current E-Business Suite used is Oracle EBS 12.1 is ERP software .The ERP server has a model no Dell PowerEdge R610 rack server .

All the 14 tertiary care hospitals across India have HIS database at unit level while the ERP is centralized.

Each HIS database has two servers: A Production Server with model no IBM System x3500 M4 and Local Standby Server.

The HIS workstations /clients at unit level are connected to the production database server where the entire clinical and non-clinical data is backed up.The 14 tertiary care hospitals units are in turn connected to centralize ERP where administrative data is backed up.There is an interface between production servers (unit level) and ERP server. Finally the ERP server is mapped with Storage Area Network (10 TB) where the entire fourteen hospitals data i.e. clinical, non-clinical and administrative data is backed up that can be restored whenever needed or in case of disaster recovery.

There is a stand-by server where copies of backups are stored, which may prove very helpful in disaster recovery.

The Tools that are provided by oracle to take backup are RMAN backup and EXPDP. Recovery Manager (RMAN) is a utility that can manage entire Oracle backup and recovery activities.

The IT team that provides its full time services support consists of 14 IT managers, 14 DBA and 2 backup and recovery system managers.

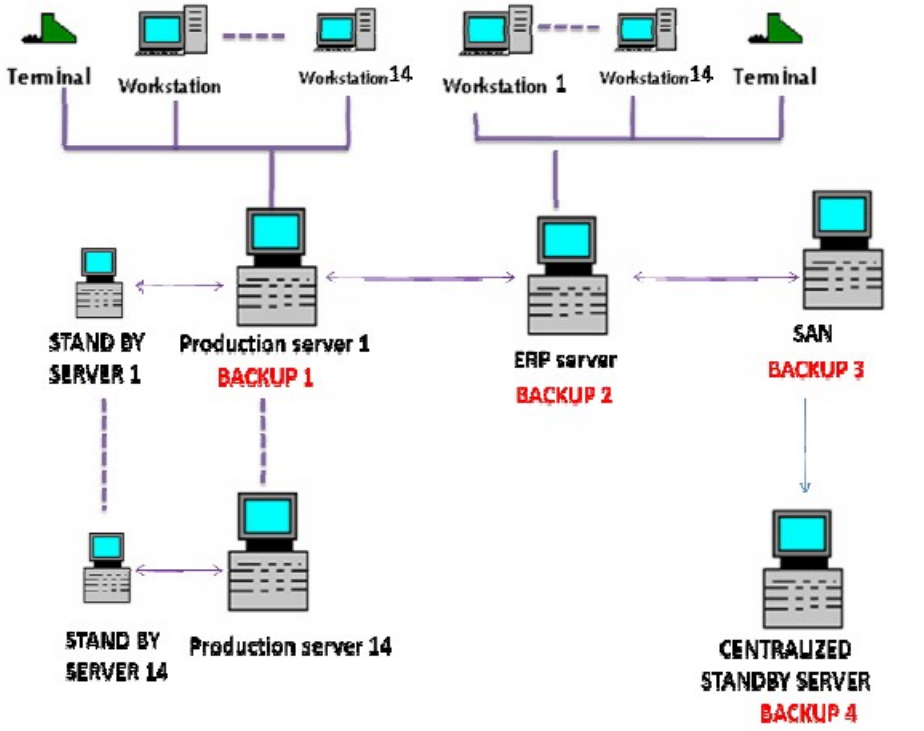

Figure 1: Sketches of the entire details of the HIS, ERP server, backup systems and SAN details

There are two types of back up strategies followed :

The Incremental Backup is designed to create backups of files that have changed since the most recent. The presence of the archive attribute indicates that the file has been modified and only files with this attribute are backed up. When a file is backed up, the archive attribute is cleared. If the file is later modified, this attribute is set, which indicates that the file needs to be backed up. It is done every day AT 4; 30 A.M.

In Full Backup method is used where all the files are backed up which includes your entire system and all the files. In each full backup session all the organizational data is copied regardless of the setting of the archive attribute. They preferred full backups because they are most comprehensive and self contained when the files are backed up, the archive attribute is cleared. If the file is later modified, this attribute is set, which indicates that the file needs to be backed up. Full Backup is carried out on every Sunday.

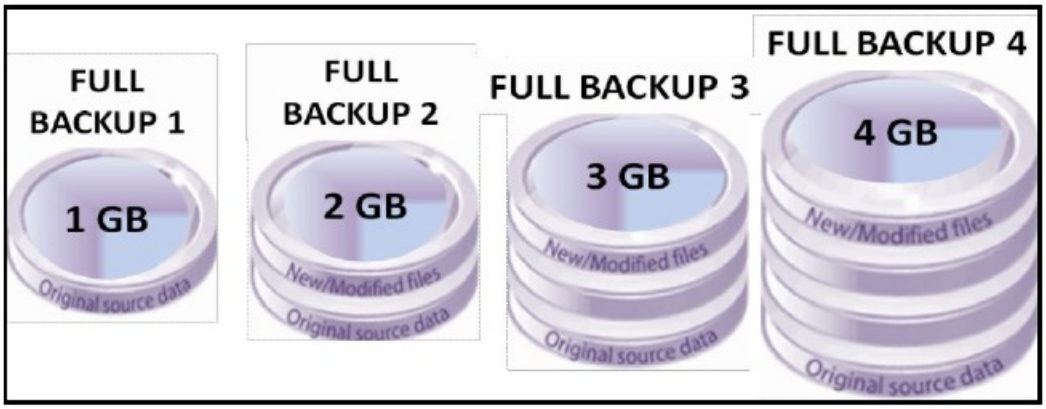

Figure 2: Full Backup Practices

The storage media used for data backup are hard drives that are added to storage area network (SAN) which is a dedicated network that provides access to consolidated, block level data storage which are accessible to servers.

The data backup and recovery system manager also maintains Offsite Backup storage where the backed up data is encrypted and stored on optical disc on monthly basis , kept in fireproof and safe Location.

The backup and recovery system is maintained by a professional vendor which is Bangalore based. The Bangalore based firm tests the proficiency of the system at least ones in a month or on requirement bases.

Testing data backup files and its ability to restore the data are tested on monthly basis. This helps the team to anticipating server failures before they actually happen.

There are totally three Disaster recovery servers one production server that generates live backup and two stand-by servers.

Production server: Servers where the data is stored as soon as it is entered.

Stand-by servers: These are the spare servers which may help in restoration of the backed up data when the production server doesn't respond.

Conclusions

Computer users are familiar with the problem of lost data such incidents may result in lost work or the deletion of unnecessary files or the nature of the lost data can be critical and the cost of lost data is significant. Information is an asset like other important business assets which is essential to an organization's business and consequently needs to be suitably protected specially in interconnected business environment. The Management should support and provide a means to backup relevant data on a regular basis. A standard hardware with a sound hospital management system can make important hospital data safer. The backup methods that are studied in the research are The Incremental Backup and Full Backup method. The entire system should be supported by good team of information technology professionals.

List of Abbreviations

- DBA- Database administrator
- EBS- E-Business Suite (Oracle Corporation)
- ERP- Enterprise Resource Planning
- EXPDP- Data Pump Export utility
- HIS- Hospital Information System
- IBM- International Business Machines
- IS - Information systems
- IT- Information Technology
- RMAN- Recovery Manage
- TB- Terabyte (1024 Gigabytes)

Reference

1. Bridgehead software report (2008), strategies to reduce the cost of managing healthcare data, UK.(www.bridgeheadsoftware.com) [Accessed on 24/01/12]

2. Coombs, F (2008), PSI Handbook of Business Security, Greenwood Publishing Group, Westport, Connecticut.

3. Jon Toiga(1989), Disaster Recovery Planning: Managing Risk And Catastrophe In Information Systems, (Yourdon Press)

4. Mugoh Leon, Ateya Ismail Lukandu, Shibwabo Bernard Kasamani,(2011), Continuous Data Protection Architecture As A Strategy For Reduced Data Recovery Time, Journal Of Systems Integration 4,Pp 54-68

5. Philip L.Wandrei (2007) , Maximizing Backup and Recovery of Data and Systems, Information Systems Control Journal , volume 3 , Pp 1-

6. Tommie W. Singleton (2011), What Every IT Auditor Should Know About Backup and Recovery, ISACA journal, volume 6, Pp 1-3