A SURVEY OF COMPUTER DATA BACKUP STRATEGIES ADOPTED BY FIRMS LISTED ON THE NAIROBI STOCK EXCHANGE

By

Patrick Kisaulu

A MANAGEMENT RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILLMENT FOR THE AWARD OF MASTER OF BUSINESS ADMINISTRATION (MBA) DEGREE, SCHOOL OF BUSINESS, UNIVERSITY OF NAIROBI.

NOVEMBER 2010

DECLARATION

This project is my original work and has not been submitted for a degree in any other university.

Signed:

…………………..……………………………………….Date…………………………………..

PATRICK KISAULU,

REG: D61/P/8030/2001

This project has been submitted for examination with my approval as a university supervisor.

Signed:

…………………..……………………………………….Date…………………………………..

J.T. KARIUKI.

DEPARTMENT OF MANAGEMENT SCIENCE,

SCHOOL OF BUSINESS,

UNIVERSITY OF NAIROBI.

DEDICATION

This study is dedicated to my family.

ACKNOWLEDGEMENT

I wish to acknowledge all those who contributed to the success of this project. Special thanks to my supervisor for his guidance and support during the entire period of the survey and to my family for their support and encouragement.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

CD-R	Compact Disk – Readable
CD-ROM	Compact Disk – Read only Memory
CD-RW	Compact Disk – Re-Writable
CMA	Capital Markets Authority
ERP	Enterprise Resource Planning
ICT	Information Communication Technology
IS	Information Systems
IP	Internet Protocol
LAN	Local Area Network
NAS	Network Attached Storage
NSE	Nairobi Stock Exchange
SAN	Storage Area Network
SPSS	Statistical Package for Social Sciences
WORM	Write Once Read Many

ABSTRACT

Continuous provision of computing services is of crucial concern to organizations that rely on computer based information systems. Organizations incur costs when computer based information system breakdown and as such they should ensure reliable backup strategies are implemented to cushion against potential loses.

The objectives of the survey were to establish the backup strategies adopted by firms listed in the Nairobi Stock Exchange (NSE), to determine the factors firms consider when selecting an appropriate backup strategy and to establish the challenges faced in implementing backup strategies.

The survey used a descriptive survey research design and was based on all the 46 firms listed on the NSE as at October 2009. A structured questionnaire with both open and closed questions was the key instrument for primary data collection. The questionnaire was administered to the Information Communication Technology (ICT) staff of the firms. A response rate of 89% was achieved with 41 out of the 46 questionnaires replying to the questionnaire. The data collected was checked for errors and completeness and then analyzed using statistical measures of mean, proportions and standard deviations

The research found that the firms surveyed had identified the critical computer data within their organizations and performed regular computer data backups. 95% of the firms contacted had a well established data backup policy. Most firms had documented their data backup procedures to guide the backup processes. Organizations reported backing up computer data on either a daily, weekly or on a continuous basis. The survey found that network based backup methods were widely used among the organizations surveyed. Tests for recoverability of backup data were undertaken on a monthly basis for most of the firms surveyed. On the factors the firms considered when selecting backup strategies the survey showed that the reliability of the backup medium, ease of use of particular backup medium, the volume of data an organization and the impact of systems unavailability to a business were the key factors that influenced the choice of a data backup strategy.

The surveyed firms reported the volume of data to be backed up, requirements for data confidentiality, and time taken for backup operations to complete as the main challenges they faced when implementing data backup strategies. Other challenges reported included systems' downtimes while backups are run, the amount of time available for backup tasks , the existence of critical data in different locations, different formats and in different operating systems environment

The survey concluded that the firms placed a high importance on computer data backups with this responsibility being undertaken by the ICT staff in most of the firms. Although the magnetic tape was still popular, majority of the firms surveyed had adopted network based backup methods. Reliability and ease of use of backup media were key factors considered by the firms in selecting particular backup strategies. The cost of the backup strategy was not a key consideration factor of the backup strategy to adopt. Large data volumes and the time data backup operations take to complete were the main challenges faced when implementing data backup strategies.

CHAPTER ONE

INTRODUCTION

1.1 Background

Organizations are increasingly reliant on computer based information systems for their transaction processing, management reporting and decision making. As a result of increased computerization, most organizations data and information are held in electronic form in computer hard disks, tape drives, compact disks and other forms of storage. No matter how well computer based information systems are designed, they often experience problems such as hardware failures, software errors or users' mistakes (Cashman et al, 2008). The simple acts of booting a computer, opening a file, adding new data on to a hard disk or running a routine maintenance program can result in data and information loss (Ngemu, 2000). Data and information loss may significantly disrupt an organization's operations as it often results in unavailability of critical information systems necessary for business operations. Organizations loose in terms of money and time spent in reconstructing the lost data and information and the negative business reputation due to interruption of business operations and services. As such, organization's data and information should be taken great care of but as Doyle (2001) points out looking after an organizations' hard disks is not enough and organizations should always keep backup copies of their data.

Data Backup has been defined as the activity of copying program files and data so that they are preserved for a period of time to safeguard against equipment failure or other catastrophe (Cashman et al, 2008). Doyle (2001) defines a backup file as a copy of a file which can be used in the event of the original file being corrupted or damaged. A periodic data backup is the most common technique used to ensure that data and information if lost can easily be recovered (Heathcote, 2000). The process of recovering lost files from a data backup is referred to as restoration.

To ensure preparedness from disasters arising from data losses, organizations adopt different backup strategies and methods. Mulhauser, G (2010) in his case study mentions backup strategies as defined around the backup media used, type of backups, frequency of backups, storage of backups, and automation of the backup process.

The backup strategies employed by a particular organization are selected taking into considerations factors such as backup media reliability, usability, storage capacity, cost, needs for data confidentiality and the nature of the business.

To implement a particular strategy organizations face certain challenges such as large data volumes, high cost, multiple locations of data, backup failures, system downtimes, lack of procedure and policies to guide the backup procedures and unavailability of staff to perform backup operations successfully.

1.2 The Nairobi Stock Exchange

The NSE is a market that deals in the exchange of securities issued by public quoted companies and the government. It was started in the 1920's by the British initially for Europeans only and in 1954 it was incorporated into a company (Exchange, 2009). The NSE facilitates the buying and selling of shares and bonds and as at October 2009 had 46 firms listed. The firms listed on the NSE are categorized by industry into Agricultural, Commercial and Services, Finance and Investment and Industrial and Allied (See Appendix 1). The contribution of the NSE to the economy is immense considering that it is the vehicle through which individual companies and the government raise capital and investors buys various instrument to invest their money. The NSE has undergone some major development on the trading and the settlement platform. These developments include the establishment of a modern and fully automated custody and settlement services through the Central Depository System Corporation (CDSC). The CDSC became operational in 2004 after decades of a manual clearing and settlement system. This was followed by a successful implementation of an Automated Trading System (ATS) in September 2006 on a Local Area Network at the trading floor. This level of adoption of ICT by the NSE itself is a reflection of the adoption of ICT by the listed firms. Most of the listed firms, due to their size and their regulation by the Capital Markets Authority (CMA) have computer based information systems. By the firms being users of computerized systems alongside regulation by the CMA, they would suffer a lot in the event of data and information loss. The firms are more likely to have in place backup measures that cushion against data and information loss. This survey therefore, sought to identify the backup methods used, factors considered in selecting particular backup strategies and the challenges faced in implementing those strategies by the listed firms.

1.4 Statement of the Problem

Organizations must ensure that critical business services and information are available to customers, suppliers, regulators and other entities on an ongoing basis. This is usually achieved by organizations developing and implementing business continuity plans. Business continuity plans are the proactive measures taken with the objective of keeping an organization up and running during interruptions of power failures, Information Communication Technology (ICT) system crashes, natural disasters, supply chain problems and more, (Slater, 2008). As part of implementing business continuity plans, organizations develop more elaborate disaster recovery plans. Disaster recovery planning is a statement of the actions to be taken before, during and after a disaster that enable an organization to resume business after a disruptive event. With respect to computer based information systems, this entails a documentation of the processes to be undertaken in backing up and in recovering failed information systems and data. With increased computerization of organizations processes, businesses' operations and reporting are reliant on computer based data and information systems. The computer based information systems should be recoverable fast in the event of a failure. Existence of a reliable and usable computer data backup is the starting point towards a successful recovery of a failed computer based information system.

Studies on disaster recovery planning and computer security have been undertaken, with the focus being mainly to gauge preparedness of organizations and to identify the aspects of information systems security considered important by organizations. Previous studies for example, Nyambura (2005) carried out a survey of the Information Communication Technology (ICT) aspects of disaster recovery considered important for firms listed in the Nairobi Stock Exchange. The survey identified data backups as one of the key ways in which organizations cushion themselves against data and information loss in the event of a disaster. Ogeto (2004) undertook a survey of computer based information systems security implemented by large private manufacturing companies in Kenya. The survey identified data backup as one of the key Information Systems (IS) security measures implemented by firms.

Data backup is therefore an integral part of ICT disaster planning and a critical element of implementing controls for computer based information systems. In analyzing the extent of ICT disaster preparedness of organizations and information system's security, studies on ICT security and disaster planning emphasize the need for organizations to ensure adequate backups of critical data are made. Nyambura (2005) noted that companies should backup all critical corporate data and information. Data and information backup plays a major role in a total system of controls and is a key element of recovery (Burch, 1979).

The emphasis on data backups hinges on the increasing use of computer based information systems to support business processing, storing and sharing of data and information. A 1995 United Kingdom survey reported by Robson (1997) established that 78 % of information systems availability was paramount for business activity to continue with 10% systems' availability being considered important.

Various studies (Ogeto (2004), Nyambura (2005), Robson (1997), Ngemu (2005)) point out the need for organizations to perform adequate backups to ensure faster recoverability and as part of an overall system of controls. These previous studies have highlighted and acknowledged the importance of computer data backups for organizations. Although these previous studies have recommended the adoption and implementation of computer data backup strategies, no previous studies have explored on the data backup methods, factors to consider in selecting a data backup and the challenges experienced by organizations when implementing the recommended backup strategies. Organizations therefore do not have information on the backup strategies adopted by organizations, the factors considered in adopting particular strategies and the challenges faced in implementing backup strategies. This information is useful in assisting organizations to map their business requirements to appropriate backup strategies. This study therefore focused on establishing the backup strategies adopted by firms listed on the NSE, the factors considered when selecting an appropriate backup strategy and the challenges faced by listed firms while implementing back up strategies.

1.5 Objectives of the survey

The objectives of this research survey were to:

i. Establish the backup strategies adopted by firms listed in the Nairobi Stock Exchange;

ii. Determine the factors firms consider when selecting an appropriate backup strategy; and

iii. Establish the challenges faced in implementing backup strategies.

1.6 Importance of the survey

The findings of this survey are beneficial to the following:

ICT professionals – to offer information on the existing backup practices by highlighting what other organizations are doing, backup methods used, challenges faced and the factors to consider in implementing particular backup strategies;

Organizational planners – the survey offers information for use in building a wider organizational disaster recovery plan; and

Researchers and academicians- the survey offers more information in the field of backup strategies with a Kenyan perspective and lay foundation for further research.

CHAPTER TWO

LITERATURE REVIEW

2.0 Introduction

Organizations differ in their extent of adoption and reliance of information systems technology and as such undertake different strategies for securing their data and information to facilitate recovery (Nyambura, 2005). There are no laws or rules to guide the backup strategies adopted by organizations and as explained in Heathcote (2000) backup practices adopted by organizations vary with respect to the backup medium used, storage of the backup medium, frequency of backups, number of backup generations held, types of backups performed and the responsibility for implementing the backup strategy.

In choosing particular backup strategies organizations consider the potential loss of revenue or operational flexibility should data and information be lost, the cost of purchasing, installing and maintaining a suitable backup solution, the time required to backup data, the ease of backing up data and the reliability of the backup media (McNamara, 2002).

To mitigate on their losses, organizations adopt different strategies to ensure existence of usable backup copies of critical data that can be successfully restored. Spafford (2005), points out that organizations backup strategies include the following considerations:

2.1 Ongoing Risk Analysis

An organization should continuously analyze the risks it faces with respect to data and information loss and their potential impact to the business. An understanding of the threats and the risks that management is willing to accept and how to mitigate those risks is vital to not only implementing a backup strategy, but also for keeping the strategy aligned with the needs of the organization (Stafford, 2005). From the results of an ongoing risk analysis, an organization should develop plans to mitigate on the potential losses.

2.2 Backup Media

Backup medium refers to the devices used by an organization to store copies of their data and information. Different backup media exist with different costs and offering different storage capacities. An organization should select the appropriate media that meets its data backup needs. French (1996) identifies magnetic disks, magnetic tape and optical disks as the media mostly used by organizations to backup computer data and information.

Magnetic Disks

These are flat rotating circular plates coated with magnetic material. Some magnetic disks are rigid and therefore, called hard disks while others are flexible and referred to as floppy disks (French, 1996). Magnetic disks differ in respect of their storage capacities, speed and cost. Doyle (2001) notes that floppy disks have inadequate storage space and are seldom used for data backup purposes. Magnetic disks are however, increasingly providing high storage capacities with high reliability. Some organizations opt to have a computer configured with additional hard disks, with one of the hard disks dedicated for backups. Another similar approach is to have a dedicated computer for backing up files. This is not an appropriate backup strategy as backup copies must be done on removable media that is then stored in a different location (Hutchinson, 1994). Magnetic media is however, nowadays packaged as removable media in the form of external disks, flash disks and zip disks thereby enabling remote storage.

Magnetic Tape

Similar to the audio and video cassette tapes, Reynolds and Stair (2008) identify the magnetic tape to be the oldest backup medium. It is a sequential storage medium which means if a computer needs to read data in the middle of the tape, it must first traverse all the tape before getting to the desired piece of data. Magnetic tapes are advantageous in that they offer low cost high storage capacity and as Stevens (2007) points out, one only needs to buy extra tapes to get more space, not extra drives. Magnetic tapes however, require a lot of time to retrieve the desired tape, mount it and traverse the tape to get to the desired data. Additionally, magnetic tapes require a lot of storage space though modern tape drives and cartridges are smaller in size.

Optical Disks

These are a direct access storage medium that is written to or read from by laser beams instead of magnetic methods as happens with magnetic media (Summer, 1995). The optical disks used with computers have been identified by Hutchinson and Sawyer (1996) as consisting of CD –ROM, CD-R, WORM and Erasable optical disks. CD-ROM is a read only memory, CD-R is rewritable, WORM are written to once and read many times whereas erasable optical disks can be erased and written over again. Though offering limited storage capacities, optical storage media is less susceptible to deterioration and contamination when compared to magnetic media (Hutchinson and Sawyer, 1994).

Network Attached Storage

Network Attached Storage (NAS) employs network devices which attach to a network instead of a single computer. The network-attached storage device is attached to a local area network and assigned an Internet Protocol (IP) address. File requests are mapped by the main server to the NAS file server. Further, NAS have software to manage storage access and file management thereby relieving individual computers of those tasks (TechTarget, 2009)

Storage Area Networks

A Storage Area network (SAN) is a special purpose high speed network that provides connection between data storage and computers in an organization. Typically, a storage area network is part of the overall network of computing resources for an organization. George and Stair (2008) note a SAN offloads the network traffic associated with storage onto a separate network. Data is then copied to a remote location thereby creating offsite backup copies. Organizations using SANs gain from reliable back-ups, smaller back-up windows and continuous business operations that do not have to stop as data gets backed up (Mohamed, 2006).

Web Based Backups

Web based backups involve the use of high-speed data lines to automatically get data backups off-site thereby enabling a restoration of the data to temporary offices anywhere. Web backups have been pitched mainly as a consumer convenience, and are ideal for small companies with few IT support resources and lacking structured backup procedures (Rubenking, 2001).

2.3 Scheduling of backups

There are no defined rules on when backups should be undertaken or the frequency of backups that an organization should adopt. A backup strategy should fit with other organizational systems and business stakeholders to determine when, how often backups can happen and how long systems can be unavailable. Hutchinson and Sawyer (2004) point out that a popular rule of thumb is to never let the time between backups go longer than the volume of data represented by that period and which volume of data, an organization is comfortable to lose in a disaster situation. As such the frequency of backups should primarily be guided by the amount of activity on a system. Managers should adopt optimal backup policies that ensure program files and data are backed up regularly.

2.4 Storage of Backups

Backups should be kept in safes that are fire proof and as Haag (2003) adds, heat proof particularly where magnetic media is used. Backup media is susceptible to water and as such it is recommended that the backup storage safes should be water proof as well. In the case of magnetic media they should be in a case or vault that is shielded from electro-magnetic radiation. Backup copies should be kept in remote locations different from their source (Hutchinson and Sawyer 1996). Seymour (2009) notes that backups kept on-site are useless when that site is burning rubble. Another approach employed by organizations is to store backups with security companies; a process known as televaulting.

2.5 Types of Backups Performed

An organization can perform either or a combination of the following backup types in implementing its backup strategy.

Full Backup

A full backup is the starting point for all other types of backup and contains all the data in the folders and files that have been selected for back up. As full backup stores all files and folders, frequent full backups result in faster and simpler restore operations; other backup types may take longer to restore. This backup type is costly in terms of effort, time and the storage capacity requirements (Backup4All, 2009)

Differential backup

A differential backup contains all files that have changed since the last full backup. The advantage of a differential backup is that it shortens restore time compared to a full backup or an incremental backup. However, if you perform the differential backup too many times, the size of the differential backup might grow to be larger than the baseline full backup (Backup4All, 2009).

Incremental backup

An incremental backup stores all files that have changed since the last full, differential or incremental backup. The advantage of an incremental backup is that it takes the least time to complete. However, during a restore operation, each incremental backup must be restored, which could result in a lengthy restore job (Backup4All, 2009).

Mirror Backups

A mirror backup is a straight copy of the selected folders and files at a given instant in time. A mirror is the fastest backup method because it copies files and folders to the destination without any compression. However, the increased speed has its drawbacks in that it requires larger storage space and it cannot be password protected (Backup4All, 2009).

2.6 Responsibility for Backups

The ultimate responsibility for proper backups rests with the data storage owner. While it is perfectly alright to delegate the task of creating the backups to other staff, it is recommended that the owner verifies that backups are being made and tested on a regular basis. (InsideStorage, 2009)

Due to its importance in a disaster recovery situation, data backup responsibility should be a concern for top management and part of an organizations policy framework. Often, this responsibility rests with ICT personnel with some organizations having dedicated backup administrators. End-users are often sensitized to ensure data held in their laptops and desktops is backed up.

Each data backup process should have at least one primary person-in-charge and one substitute. Data backup is a critical disaster planning and security measure and as such, the relevant persons responsible should be committed in writing to adhere to the specific data backup policies and procedures.

2.7 Retention of Backups

A backup strategy should work together with other systems, business and legal stakeholders to determine how long data should be retained.

To minimize on the risk of data and information loss, an organization should retain copies of its backups for longer periods. It may be useful to establish a hierarchy of backup cycles. For instance, a five-generation full daily backup cycle might involve retaining five sets of backups –one for each working day. The fifth daily backup is then retained for one month, as part of a weekly backup cycle and stored in a local safe. Finally, the fourth weekly backup might be retained for one year as part of a monthly backup cycle and stored in the off-site backup archive storage location. Annual data backup should be generated in multiple copies and each copy stored in a distinct archive storage location. This way, the risk of data and information loss is considerable minimized and chances for a quick recovery are increased.

2.8 Backup Logs

A good backup strategy should include the maintenance of backup logs and their review. Backup logs are useful for reviewing backup activity to ensure the frequency and completeness of backup processes. Log files generated from each backup job should be reviewed to check for errors, duration of the backup job and so on. On identifying problems with the backup logs, corrective action should be taken to reduce any risks associated with failed backups.

Auditors often fall back to backup logs to ensure that backups for critical data are maintained and the logs are reviewed (Stafford, 2005).

2.9 Backup Disposal

Backup media often need to be disposed of when it becomes un-usable or the data contained therein is no longer required. Such media should be physically destroyed to ensure that their contents are not accessible to unauthorized persons.

2.10 Backup Testing

Organizations should undertake a test of their backup equipment, media and processes to ensure that these are working and reliable for use in a recovery situation (Computer Associates, 2005). Backup testing is important in ascertaining the recoverability and the amount of time required to restore data.

As Stafford (2005) explains, it is far better to find out the causes and take corrective action in the safe confines of monthly or quarterly testing than it is in the heat of battle.

2.11 Factors Considered in Selecting Backup Strategies

Organizations take into consideration various factors when selecting the backup storage methods to use. In making this selections, Reynolds and Stair (2008) notes that organizations should select a type of backup storage based on their needs and resources. The following are factors organizations consider in selecting particular backup strategies.

Reliability

A backup medium must be able to hold data without corruption for years. McNamara (2002) notes that the decision as to which backup strategies are appropriate for an organization is guided by the life span of the backup media. The way the medium is used and stored affects its reliability as a backup medium. A hard disk is typically very reliable, but as a backup medium it is not very reliable, if it is in the same computer as the disk you are backing up. Optical media as noted in Hutchinson (2004) are less susceptible to deterioration and contamination compared to magnetic media. Kendall and Kendall (2007) note that organizations are moving to Storage Area Networks to get away from the unreliability associated with physical tape backups and storage. A March survey by the Yankee Group and Sunbelt Software found that 40% of IT managers had been unable to recover data from a tape when they needed it (TechTarget, 2009).

Usability

A backup method should be easy to use and implement and often the ease of use of a particular backup method influences the frequency with which backups are made. Magnetic tapes usually present challenges in view of the time and effort required in mounting and accessing data. Certain optical disks such as CD-R have the disadvantage of writing data permanently and as such the media cannot be re-used by overwriting older backups (French, 1996). However, optical disks nowadays can be re-written. Another trend towards better usability is backup automation through backup scheduling. Various software such as NovaStor assist in locating the files to be backed up and in scheduling when these files should be backed up (American University of Beirut, 2009).

Organizations should adopt solutions that leverage backup to disk so as to minimize the need for end user involvement in tape handling, backups for remote locations and disconnected clients. This should be integrated with tape based infrastructure at centralized locations to take advantage of very low cost storage over time.

Storage Capacity

Organizations differ in their extent of adoption of ICT and consequently, the amount of data they generate (Nyambura, 2005). Different backup media in turn differ in the volumes of data they can hold and as Reynolds and Stair (2008) pointed out, storing large amounts of data and letting users access it quickly makes an organization more efficient. Individual organizations will therefore acquire particular backup media to match their data needs. An organization should choose the media that meets current and future data demands.

Cost

Backup cost can be looked at in terms of the cost of the investment and time taken to perform backup tasks. McNamara (2002) points out that the cost of purchasing, installing and maintaining a suitable backup system as a major determinant of the backup methods chosen by an organization.

Different backup media have different costs with Network Attached Devices and Storage Access Networks being the more expensive to implement and run. A cheap medium is usually the best to ensure adequate backup copies are retained for relatively long periods. The administrative expertise and offsite storage locations required to implement a backup strategy are expensive to acquire and maintain and organizations should evaluate the optimal investment costs (Bitpipe, 2009).

Data Confidentiality

Where an organization chooses to use web based backup methods, it must be comfortable that the transmitted data is secure and the organization offering the storage facilities can be relied upon to hold data confidentially (Stevens, 2007). Within organizations, staff must be comfortable that sensitive data backed up is securely kept and accessible to authorized persons only. The need to ensure backup data is secure influences the backup strategies adopted particularly with respect to data backup storage.

Nature of business

Due to their nature and extent of reliance on information systems for business operations, data and information loss will present different challenges to particular organizations. McNamara (2002) points out that organizations choice of data backup methods will be influenced by the potential loss to the business and the effect on operational flexibility should data and information is lost. Organizational structure with respect to branch networks will also help define offline storage options adopted by organizations. Where an organization is housed in one building, it may have to consider outsourcing offsite data backup storage to security companies.

2.12 Challenges in Implementing Backup Strategies

An appropriate backup solution should provide for rapid, reliable and comprehensive restore of important systems and data to appropriate recovery points. The solutions adopted by an organization should also be cost effective and easy to use.

Slow Backups

One of the challenges faced by ICT professionals when performing data backups is the time taken to perform backup operations. Various reasons exist for slow backup performances but often this has to do with increased size of critical backup data as an organizations data files grow. Another reason for this is limited or lack of dedicated staff for data backup administration with the possibility of just one ICT staff responsible for all operations (Bitpipe, 2009). Different backup media present different backup speeds with tape backups considered slow due to their sequential access. To counter speed related problems, organizations should strike a balance between disk and tape backups so as to take advantage of the fast access speeds of disk backups while leveraging on high storage capacities offered by tapes.

Cost

As organizations data grows, the backup storage requirements of organizations increase. Applications such as Enterprise Resource Planning (ERPs), Email software tend to require a lot of backup space. Stevens (2007) notes that price is a major consideration for organizations in choosing to adopt particular backup strategies. One way of reducing backup costs is by blending disk and tape usage appropriately thereby leveraging disk advantages (random access) and tapes advantage (low cost storage) to achieve optimal cost while improving overall recoverability and reliability.

Backup storage is costly in terms of the cost of disk storage, safes and establishment or acquisition of offsite storage locations. Online backup services are expensive in terms of the cost of storage space and bandwidth required to transmit the data (PC Magazine, 2006). Due to these cost elements, an organization may fail to implement proper backup strategies thereby exposing itself to data and information losses in the event of a disaster (McNurlin and Sprague, 2006).

Multiple Locations of data

With the proliferation of computers, end users are increasingly empowered to generate organizational data in the form of documents at their desktops and laptops some of which are not networked. A lot of corporate information is housed in users’ computers rather than in the data center. Some of this information is critical to the organization and should be backed up often. Further, organizations are increasingly having critical data in different platforms such as Linux, windows, Unix or Netware (Bitpipe, 2009). For ICT professionals dealing with many users, the backing up data stored in many locations poses challenges with respect to identifying and ensuring all relevant data is included in backup files. Nyambura (2005) identifies lack of information on critical systems and applications of an organization as one of the challenges faced by organizations implementing disaster recovery plans.

Backup Failures

Often backup operations fail to complete or on completion will have excluded certain critical files due to inability to access the files that need to be backed up. Backup media or the backup files could also fail at recovery time. In a survey of five hundred IT departments completed in January 2004, Meta Group found that as many as 20% of routine, nightly backups fail to capture all data. (Regan, 2004). French (1996) points out that magnetic medium are susceptible to heat, stray magnetic fields and dust and therefore cannot be relied upon to hold data indefinitely. Organizations should have backup procedures that include periodic testing of backup files for recoverability and completeness.

System Downtimes

Backup operations often consume large computing resources as files are compressed and copied on to backup media. This significantly affects the processing capabilities of the backup clients or servers. If performed at server level, backup operations can slow shared applications due to the increased competition for system resources. Depending on the computing resources available, certain applications may become unavailable or slow during backup operations forcing users to have to wait for backup operations to complete. This introduces costly system downtime with organizations resulting to running backups during off peak times.

Lack of Policies and Procedures

Organizations should have backup policies and procedures to guide the implementation of selected backup strategies. These policies should include a definition of the critical data and information to be backed up, storage, frequency and the procedures for creating backups. Nyambura (2005) identified lack of policies and procedures to guide data backups as one of the reasons organizations fail to implement appropriate disaster recovery plans.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Research Design

This research involved a survey of the data backup strategies adopted by firms listed on the Nairobi Stock Exchange. Data was collected on the backup strategies adopted by these firms, the factors considered in selection of backup strategies and the challenges commonly experienced when implementing backup strategies. The data collected in the survey was analyzed out using Statistical Package for Social Sciences (SPSS) software.

3.2 Population

The population of the survey consisted of all the firms listed on the NSE. As of October 2009, the time when the survey was undertaken, there were forty six (46) firms listed on the Nairobi Stock Exchange. These companies are listed on Appendix 1.

3.3 Data Collection

The survey used primary data collected through a questionnaire with open and closed questions. The questionnaire was divided into four sections. Section A of the questionnaire was used to collect data on the respondents and their organization’s profile whereas Section B collected data on the backup strategies employed by the organizations. Section C collected data on the importance the organizations attached to the list of factors considered in selecting particular backup strategies and methods. Section D collected data on the extent to which organizations rated the challenges of implementing various backup strategies.

The questionnaire was administered to the ICT staff responsible for data backup in the respective firms. The questionnaire was administered through a “drop and pick-up later” method for companies within Nairobi and by way of electronic mail for firms outside Nairobi.

3.4 Data Analysis

Descriptive statistical measures such as frequencies, means and standard deviations were used to analyze the data collected under Section A aimed at capturing the organizations’ background. Data collected in the remaining sections was analyzed using proportions, mean scores and standard deviation. Data collected in section B aimed at capturing the backup strategies used in the study organizations. Question items under this section were analyzed using proportions, mean scores and standard deviation. Data collected under Section C of the questionnaire was tabulated using a five level Likert scale. In this section, users were asked to indicate their level of agreement to the factors considered in selecting data backup strategies.

CHAPTER FOUR

DATA ANALYSIS AND FINDINGS

4.1 Introduction

This section provides an analysis of the data collected in the survey. The data collected was checked for errors and completeness. It was then coded and entered in SPSS software for analysis. Data was then analyzed using means, standard deviations and proportions. The analysis results are presented in tables, pie charts and graphs. A total of 46 questionnaires were sent out and 41 responses were received. The surveys' findings are presented in the following subsequent sections.

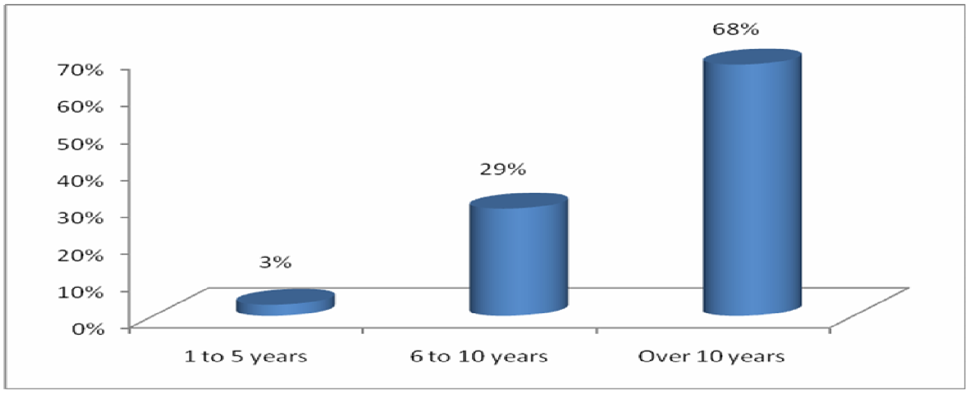
4.2 Organizations' profile

Information about the organizations' was collected for a better understanding of the firms participating in the survey. Respondents in these organizations were asked to provide information pertaining to their organizations and the results are presented in sections below.

4.2.1 Duration of use of computer based information systems

The duration of use of computer based information systems by an organization is an important factor in determining the level of adoption and development of ICT and can influence, the backup strategies adopted. The results presented in Figure 4.1 show the duration in years the firms had used computer based information systems.

Figure 4.1: Duration of use of computer based information systems

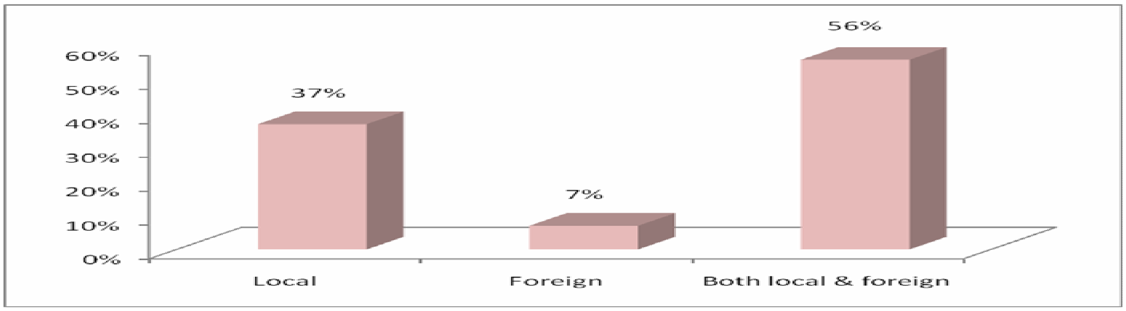


The survey established that 68% of the organisations had used computer based information for over 10 years, 29% had 6-10 years of use of computer based information. Only 3% of respondents ackowldeged usage of computer based information in their organization for periods of between one to five years. This shows a high reliance on computer based information systems by the firms under the survey.

4.2.2 Organisations' ownership structure.

This section of the survey sought to describe the ownership structure of the organization under the survey. The results presented in Figure 4.2. Show the distribution of the firms surveyed in terms of their ownership structures.

Figure 4.2: Organizations' ownership



The survey revealed that 56% of the organisations under survey were jointly owned by local and foreign investors , 37% of the firms were locally owned with the remaining 7% of the firms being owned by foreign investors. The results show that majority of the firms under survey had local ownership.

4.2.3 Organization's sector of operation

The NSE categorised organisations based on the industry in which they operate. The following is the distribution of the firms into the industry categories.

Table 4.1: Percentage distribution of organizations by sector.

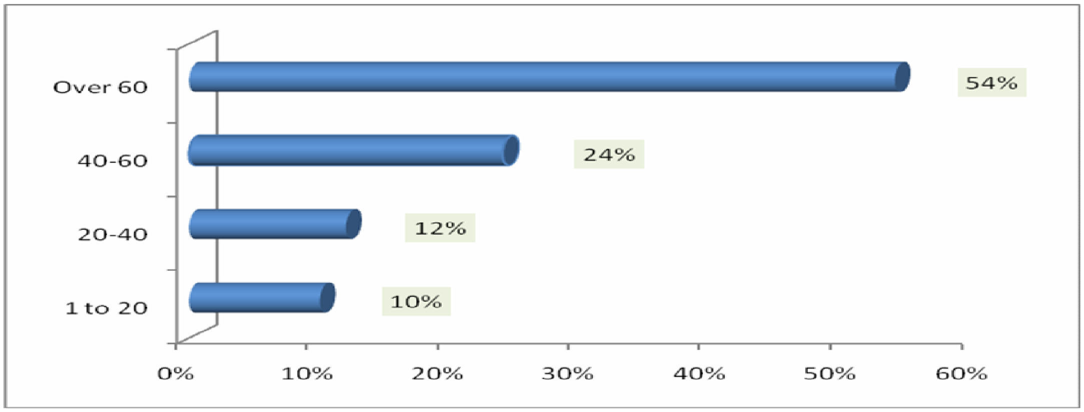
Organizations' sector of operation	**Distribution**	
	Frequency	Percent
Agriculture	1	3
Commercial and services	10	24
Financial and Investment	13	32
Industrial & Allied	17	42
Total	**41**	**100**

The results in Table 4.1 show that 42% of the organisation that responded were under industrial and allied sector , 32% financial and investment and 24% commercial and services.

4.2.4 Organisations' number of computer users

The number of computers users within each of the organisations under survey was established and the results were as presented in Figure 4.3

Figure 4.3: Number of computer users



The survey's results indicated that 78% of the organisations had over 40 computer users with only 10% having between 1-20 computer users. Additional information on the number of ICT staff in the organisations' respective ICT department showed that most of the organisation (42%) had between 1-4 staff within the ICT department, 27 percent had over 25 staff with less than 1% of the organisation having between 15- 24 staffs in their respective ICT department . the results show that the firms surveyed had a large number of computers with 54% having over 60 computers. This could also imply large volumes of computer data held by the firms.

Table 4.2: Number of staff in ICT department

No of Staff	Distribution	
	Frequency	Percent
1 to 4	17	42
5 to 9	5	12
10 to 14	4	10
15 to 20	1	2
20 to 24	3	7
Over 25	11	27
Total	**41**	**100.0**

Majority of the firms surveyed did not have a large number of ICT staff. However, a significant 27% of the firms had over 25 ICT staff.

4.3 Backup strategies adopted by organisations

Data backups are used to ensure that data and information if lost can easily be restored. The strategies adopted by organizations vary a great deal and one of the objectives of the survey was to establish the backup strategies adopted by the various organizations.

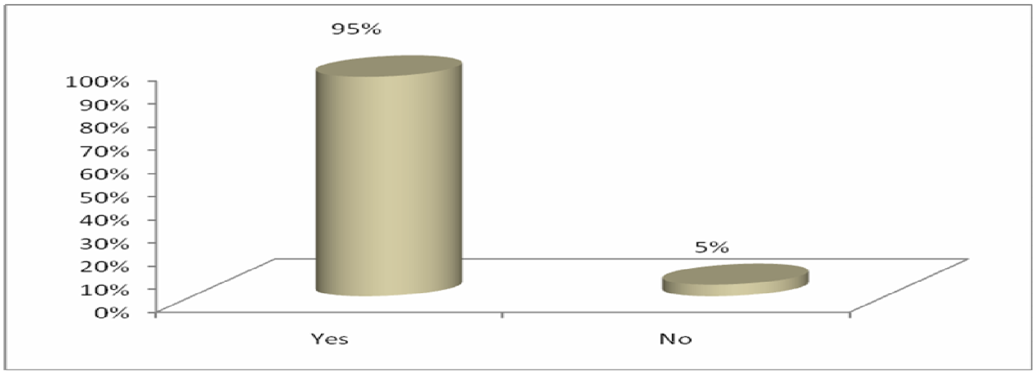
4.3.1 Identification of critical data to organisation and regular backups

Organizations should ensure all critical data is identified and regularly backed up. The survey sought to establish the extent to which the organizations surveyed had identified critical data in their organizations and the frequency with which critical data is backed up. All the respondents in the survey have critical computer data within their organizations identified and regularly backed up. This shows a high concern for data backups within the organizations surveyed.

4.3.2 Existence of data backup policy

Data backup policies are guidelines set out by an organisation to aid in implementing data backup strategies. The survey sought to establish the existence of a documented data backup policy within the organisations in the survey . Results were as represented in the Figure 4.4 below

Figure 4.4: Existence of a data backup policy within the organizations.



The results show that largest proportion (95%) of the organisations surveyed had well established data backup policies as opposed to a minority 5% who did not have data backup policy. The results emphasize the importance attached to data backups by the organisations in the survey.

4.3.3 Documentation of backup procedures

Tables 4.3: Organizations' documentation of backup procedures

Documentation of backup procedure	**Distribution**	
	Frequency	**Percent**
Yes	39	95
No	2	5
Total	**41**	**100.0**

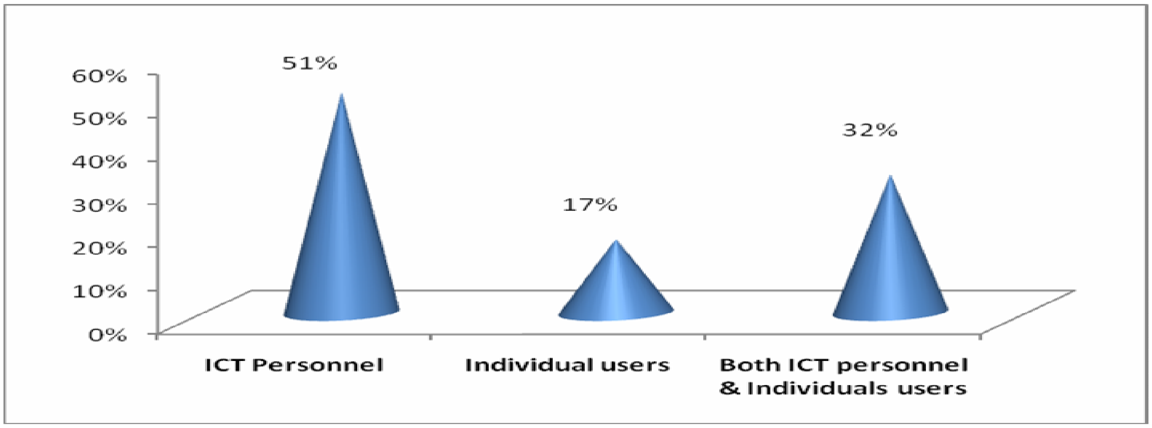
Table 4.3 shows that 39 out of the 41 respondents had documented data backup procedures with only two respondents confirming the non existence of documented data backup procedures in their

organization. A large proportion of the respondents had documented their data backup procedures, which suggests that a majority of the organizations placed a lot of importance on data backups.

4.3.4 Persons responsible for computer backup

The responsibility for data backups is entrusted to different individuals for different organizations. This part of the survey sought to establish the staff entrusted with data backup responsibilities. Results of the survey are shown in Figure 4.5.

Figure 4.5: Staff responsible for computer backup



The results of the survey presented in Figure 4.5 show that ICT personnel undertook backup responsibilities in 51% of the firms surveyed. 32% of the organizations have the responsibility for data backup shared by both ICT personnel and individual users with 17 % of the respondents indicating that data backup was a responsibility of individual users. These results show that data backup is mostly an ICT personnel responsibility but in some firms it is undertaken by the users.

4.3.5 Frequency for Computer data backup

Respondents were asked to indicate the frequency of data backup within their organization. The results are presented in Table 4.4.

Table 4.4: Frequency of data backup

Data Backup Frequency	**Distribution**	
	Frequency	**Percent**
Hourly	3	7%
Daily	25	61%
Weekly	6	15%
Monthly	1	2%
Continuous	6	15%
Total	**41**	**100**

More than 90% of organizations that responded perform backups on either a daily, weekly or on a continuous basis. Results show that majority (67%) of the organizations backed up information on a daily basis, 15% on a weekly basis and 6% on continuous basis. The results show that organizations are keen to reduce on the amount of data that could be lost if systems failed with a majority either performing continuous, hourly or daily backups.

4.3.6 Medium for backup data in organization

Table 4.5 Organizations medium of data backup

Backup Media	**Distribution**	
	Frequency	**Percent**
Magnetic tape	17	41.5
Magnetic disks	24	58.5
Total	**41**	**100.0**

Findings on the medium used for backup indicated that 59% of the respondents used magnetic disks for their data backup while 41% of the respondents backed up their data to magnetic tapes. The results show the magnetic disks as the most popular media for backup.

4.3.7 Network backup method usage

The survey sought to establish the use of network backup methods among the organizations surveyed. Results showed that 85% of respondents use network backup methods in their organizations. These respondents were also asked to identify the particular network backup method employed in their organization. Results were as shown in Table 4.6

Table 4.6: Network backup methods employed

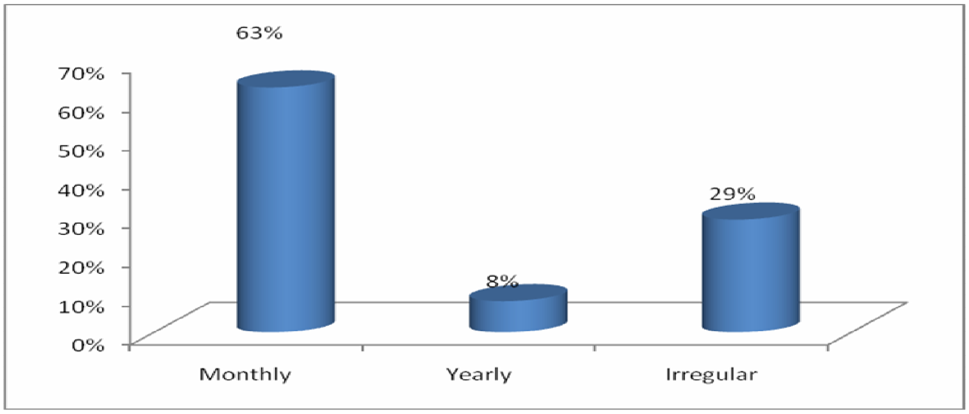
Network Backup Method	**Distribution**	
	Frequency	**Percent**
Network attached storage(NAS)	29	71%
Storage area network(SANs)	9	22%
Web based backups	3	7%
Total	**41**	**100.0**

The survey revealed that network attached storage was the most widely used method of network backup methods. This was followed by storage area networks which were used by 22% of the respondents and web based backups which were used by 7% of the respondents.

4.3.8 Tests on recoverability of backup

The viability of backup strategy must be routinely tested for data recoverability to gain comfort that backed up data can be used in a recovery situation. The survey sought to establish if the organizations surveyed tested backup data for recoverability. It was observed that ninety five percent of the respondents tested backup data for recoverability. Further, the survey sought to establish the frequency with which tests of recoverability of backup were carried out and the survey results are in Figure 4.6.

Figure 4.6: Frequency of test of recoverability of backup data

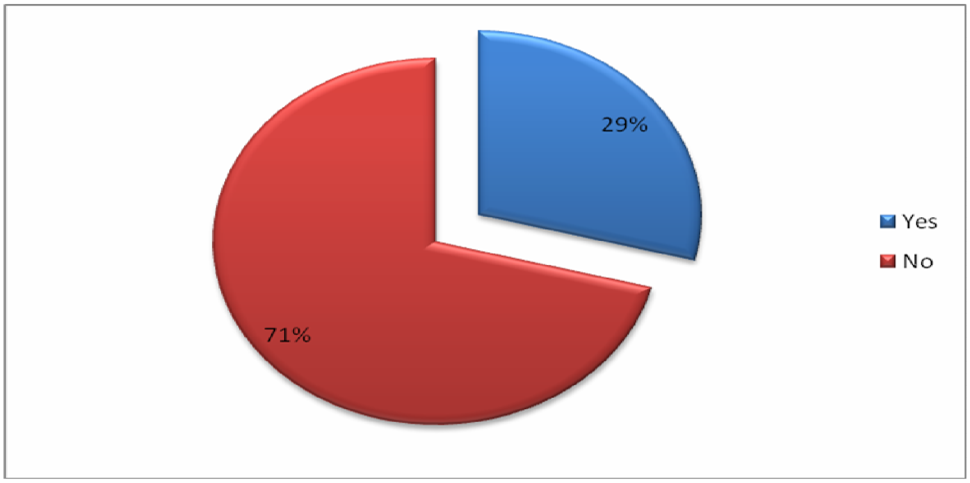


Results in Figure 4.6 above show that majority 63% of the respondent organizations tested recoverability of their backups monthly while 29% tested the recoverability of backup data irregularly. 8% of the respondents test recoverability of their backup data yearly. The results show that the firms surveyed were concerned about the usability of data backups and therefore tested for recoverability.

4.3.9 Maintenance of backup logs

Majority (95%) of respondents reported that their organizations maintained backup logs. 71% of the respondents did not physically destroy unwanted copies of backup media as shown in the Figure 4.7

Figure 4.7: Physical destruction of unwanted copies of backup media



Key: Yes – represents respondents who physically destroy unwanted backup copies

No – represents respondents who do not destroy unwanted backup coipes

The results of the survey show that majority of the firms do not physically destroy unwanted copies of backup. This could imply that the backup files are deleted from the media which is then otherwise disposed.

4.4 Factors to consider in selecting a backup strategies

The mean score for each factor considered in selecting a data backup strategy were analyzed on a Likert scale. The responses from the survey were given values based on the following scale and the mean for each factor computed.

Extremely Important (1), Very Important (2), Important (3), Somewhat Important (4), Not Important (5)

The mean scores obtained from a scale “Extremely important” and “Very Important” represented the factors considered most critical in selecting a backup strategy for an organization.

On a continuous Likert Scale ‘Extremely Important ‘and “Very Important” (abbreviated as VI), were set to be equivalent to a mean score in the range of 1 to 2.5 (1≤ VI≤ 2.5).

The scores of ‘Important’ (abbreviated as I), represented factors regarded as important in selecting a data backup strategy. This was set to be equivalent to mean score in the range of 2.6 to 3.5 on the Likert scale (2.6≤ I ≤3.5).

The score of “Somewhat Important” and “Not Important” (abbreviated as SI) represented factors that were considered least important in selecting a data backup strategy by the firms surveyed. These were set to be equivalent to a mean score in the range of 3.6 to 5.0 on the Likert Scale (3.6≤ SI≤5.0).

Table 4.7: Factors to consider in selecting backup strategies

Factor	N	Min	Max	Mean	S. D
Reliability of backup medium	41	1	3	1.20	.511
Ease of use of backup medium	41	1	2	1.34	.480
Volume of data the organization generates	41	1	3	1.34	.575
Impact of systems un availability to the business	41	1	4	1.39	.737
Requirements of data confidentiality	41	1	4	1.46	.925
Manual versus automated backup process	41	1	4	1.59	.921
Capacity of particular backup medium	41	1	4	1.63	.767
Computer Network infrastructure	41	1	3	1.78	.725
Nature of business	41	1	5	1.85	1.174
Extent of centralization of information	41	1	4	1.85	.937
Frequency of generation of data/transactions	41	1	4	1.90	.889
Cost of the backup method	41	1	4	2.05	.999
Industry and other regulatory requirements	41	1	4	2.05	1.048
Data modification times(online versus batch)	41	1	4	2.17	.998
No of systems' users in the organization	41	1	5	2.22	.936
Restoration times associated with particular strategies	41	1	5	2.34	1.277

From the results above, majority of the respondents in the organizations surveyed considered most the factors provided as either extremely important or as very important. Reliability of the backup medium (1.20), Ease of use of backup medium (1.34), Volume of data the organization generates (1.34) Impact of systems unavailability to the business (1.39) were the factors considered critical in selecting a data backup strategy. The restoration times associated with particular strategies (2.34), the number of computer users in the organization (2.22), Data modification times (online versus batch) (2.17) were the factors least considered in selecting a data backup strategy.

4.5 Challenges to computer data backups

This objective of the survey aimed at establishing challenges the surveyed firms experienced when implementing data backup strategies. The respondents were asked to rate their extent of agreement to the challenges below. The following scale was used on the responses and in computing the Mean and Standard Deviations represented below. *Strongly Agree (1), Agree (2), Neither Agree or Disagree (3), Disagree (4), Strongly Disagree (5)*

Table 4.8: Challenges to computer data backups

Challenge	**Mean**	**Std. Dev**
Volume of data to be backed up	1.22	.419
Requirements for data confidentiality	1.22	.419
Systems downtime while backups are run	1.59	.631
Critical data exists in different locations	1.61	.703
Critical data exists in different formats/operating systems environments	1.66	.656
Time taken for backup operations to complete	1.46	.636
Inadequate definition of critical data	1.88	1.029
Cost of an effective backup plan	1.76	.943
Backup restoration times	1.98	.851
Inadequate personnel for data backup	2.46	1.267
Failure of backup media	1.80	1.100
Lack of policy and procedures to support backup procedures	2.32	1.254
Poor electric power environment	2.12	1.382
Lack of top management support	2.68	1.254
Limited offside storage options	2.39	1.243
User resistance with respect to data in their computers	2.63	1.135
Inadequate knowledge and data backup competence of users	2.12	1.229
Inadequate time availability for backup tasks	1.86	1.020

Lack of clear responsibilities for backup	3.88	1.652
Lack of outsourced backup services	3.93	1.706

Results in Table 4.12 shows that firms had as key challenges to implementing data backup strategies the volume of data to be backed up (1.22), requirements for data confidentiality (1.22), time taken for backup operations to complete (1.46). This was followed by challenges of systems downtimes experienced while backups are run (1.59); existence of critical data exists in different locations (1.61), formats and operating systems environments (1.66) and inadequate time availability for backup tasks (1.86). The challenges least experienced by the firms included poor electric power environment (2.12), inadequate knowledge and data backup competence of users (2.12), lack of policy and procedures to support backup procedures (2.32), and inadequate personnel for data backup (2.46).

CHAPTER FIVE

SUMMARY, CONCLUSSIONS AND RECOMMENDATIONS

Introduction

The survey conducted sought to establish the backup strategies adopted by firms listed on the NSE, to determine the factors firms consider when selecting an appropriate backup strategy and to establish the challenges faced in implementing computer data backup strategies. This chapter presents the findings and conclusions of the study and recommendations for further studies.

5.2 Summary of findings

The survey reported a majority (68%) of the organisation had over 10 years of use of computer based information, with 29% having between 6-10 years of use of computer based information. This showed that firms under the survey had used computer based information systems for a failry long period. As regards ownerhip, 56% of the firms under the survey were jointly owned by local and foreign investors.

Most of the firms (42%) surveyed were under industrial and allied sector, with 32% under financial and investment sector and 24% commercial and services sectors of the NSE. The survey results showed that seventy eight percent of the organisations had over 40 computer users with only ten percent having between 1-20 computer users . Survey results on the number of staff in firms' respective ICT departments established that most of the organisation (42%) had between 1-4 staffs within the ICT department ,27 percent had over 25 staffs on the other hand less than 10 percent of the organisation had between 15- 24 staffs in their ICT department

On the backup strategies adopted, the respondents in the survey reported that critical computer data within their organizations was identified and regular data backup were performed in their organizations. 95% of the firms surveyed indicated that their organisations had a well established data backup policy. 39 out of 41 respondents confirmed that their organization had a well documented back procedure. Findings showed that in 51% of the firms, ICT personnel were entrusted with data backup responsibilities with 32% of the firms entrusting the responsibility for data backups to both ICT personnel and individual users. Majority (67%) of the firms confirmed backing up information on a daily basis, with 15% equally backing up their data on a weekly or on continuous basis. Findings further showed that 59% of the firms used magnetic disks for their data backup.

85% of the respondents acknowledged use of a network backup method. Network attached storage was the widely used method of network backup method followed by storage area network. Ninety five percent of the respondents reported regularly testing the recoverability of their backup. It was also observed that respondents tested recoverability of their backups on a monthly basis. Majority (95%) of respondents reported that their organizations undertook maintenance of data backup logs. Majority (71%) of respondents did not physically destroy unwanted copies of backup media

Findings on the factors to considered when selecting a backup strategies showed that the critical factors to considered were the reliability of the backup medium, ease of use of particular backup medium, the volume of data an organization and the impact of systems unavailability to a business. The least three factors considered were an organizations' industry and other regulatory requirements, computer network infrastructure, and number of systems' users in the organization.

The survey revealed that firms had the following as their major challenges to implementing computer data backup strategies; large volume of data to be backed up, requirements for data confidentiality, and time taken for backup operations to complete. This was followed by systems downtimes while backups are run, the existence of critical data in different locations and in different formats/operating systems environments and inadequate time availability for backup tasks.

5.3 Conclusion

From the survey, the following conclusions were made.

Firms had adopted different data backup strategies with the data backup responsibilities largely entrusted to ICT personnel in most organizations. The Magnetic tape as a backup medium was still popular in most organizations with a few organizations having adopted network based backup techniques. Tests for data recoverability were found to be irregularly carried out across the organizations.

The surveyed firms considered the reliability of the backup medium, ease of use of particular backup medium, the volume of data an organization and the impact of systems unavailability to a business when choosing a data backup strategy. Cost of a backup strategy was not a major factor influencing the choice of backup strategy.

The survey found that the firms had experienced challenges in implementing computer data backup strategies. Among the major challenges encountered were; the volume of data to be backed up, the requirements for data confidentiality, and time taken for backup operations to complete. Systems downtime while backups are run, existence of critical data in different locations, formats or operating systems environments and unavailability of adequate time to perform backup tasks.

In conclusion, the surveyed firms placed a high importance on data backups as a measure to ensure recoverability in the event of data and information loss.

5.4 Recommendation

The following recommendations were made based on findings and conclusions of the research survey.

It is recommended that organizations consider extending the roles of data backup to dedicated data backup staffs leaving the other ICT staff to carry out support other ICT tasks in order to promote efficiency in data backups as well as reduce data loss and system down time while backup are run.

Organizations should document their data backup procedures to ensure that clear guidelines for backup operations exist for those implementing this important task.

Organizations should also consider investing in network based backup methods to increase data availability and promote efficiencies in data backups.

5.5 Limitations of the survey

This survey was not without limitations and the following challenges were encountered.

Time allocated for this survey was limited. Respondents took long time to fill in the questionnaire and the researcher had rush against the scheduled survey time.

Some respondents were not cooperative and therefore could have given misleading information due to nature and sensitivity of the survey.

5.6 Recommendations for further research

This survey focused on companies listed on Nairobi stock exchange and therefore may not be representative of all other large organization especially in private sector. Future research studies could focus on other private institution. The research can also be extended to cover home users.

Other research areas could focus on computer based information system failures and recovery from those failures.

REFERENCES

Cashman et al (2008). **System Design and Analysis**, Fifth Edition, Boston, Thomson Course Technology.

Cummings et al (2003). Management Information Systems for the Information Age, Third Edition, Boston, Burr Ridge, McGraw Hill Irwin.

Cooper, R.D. & Schindler, S.P. (2003). Business research methods. (8th ed). Mc Graw- Hill Irwin, New York.

Doyle, S (2001). **Information Systems for You**, Third Edition, Delta Place, UK, Nelson Thornes.

Heathcote, P (2000). **'A' Level ICT**, 2nd Edition, United Kingdom, Payne Gallway Publishers ltd.

Hutchinson, S and Sawyer, S (1994). **Computers and Information Systems**, 1994-1995 Edition, Boston, Burr Ridge, Richard D. Irwin inc.

Kendall and Kendall (2007). **Systems Analysis and Design**, Seventh Edition, Upper Saddle River, New Jersey, Prentice Hall.

Mulhauser, G (2010). One example of a (hopefully) sound backup strategy, Cancelling Resource, [online], Viewed on 15/10/2010, Available at http://counsellingresource.com/practice/security/backup-case-study.html

McNamara, K (2002). **Data Backup Methods**, Radioonline Magazine, [online], Viewed on 05/04/2009, Available at http://radiomagonline.com/mag/radio_data_backup_methods/

McNurlin, B and Sprague, R.(2006). Information Systems Management in Practice, Seventh Edition, New Jersey, Prentice Hall.

Mohamed, A (2006). Data Recovery: Eliminate the weak links in data backups, Computer Weekly, [online], viewed on 05/04/2009, available at http://www.emeraldinsight.com/0010-4787.htm

Ngemu, A (2005). A Survey of Computer Forensic Practices in Litigation Support. The **Case of The Banking Industry in Kenya**, Unpublished MBA Research, University of Nairobi.

Nyambura, A. (2005). A Survey of ICT aspects of Disaster Recovery Among Companies Quoted in the Nairobi Stock Exchange, Unpublished MBA Research, University of Nairobi.

Ogeto, V (2004) A Survey of Computer Based Information Systems Security Implemented by Large Private Manufacturing Companies in Kenya, Unpublished MBA Research, University of Nairobi.

Regan, K (2004), Security News: Concerns raised on tape backup methods, Information Security magazine [online] , viewed on19/06/2009, available at http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci959858,00.html

Reynolds, G and Stair, R (2008). **Principles of Information Systems**, Eighth Edition, United States, Course Technology.

Richards, M. (2001), Computer Backups: Preventing a customer relations disaster, Inside Self Storage [online]. Viewed on 10/03/2009, Available at http://www.insideselfstorage.com/articles/141Tech.html

Robson, W (1997). **Strategic Management & Information Systems**, Second Edition, Essex, Prentice Hall.

Rubenking, N, (2006), **Buying guides: Online Backup Services**, PC magazine [online], 1962374, Viewed 29/02/2009, Available at: http://www.pcmag.com/article2/0,2817,1962374,00.asp

Seymour, J (2001). **Recovery: It's Our Job now**, PC Magazine, [online], 2/0, Viewed 02/03/2009, Available at: http://www.pcmag.com/article2/0,2817,1659218,00.asp

Slater, D (2009). **The Basics of Business Continuity Planning**, CSO Online, [online], Viewed on 28/08/09 Available at http://www.csoonline.com/article/204450/Business_Continuity_and_Disaster_Recovery_Planning_The_Basics)

Stafford, G (2005). **Backup, Best Practices Save Critical Data**: Datamation, Viewed on 19/07/09, Available at http://itmanagement.earthweb.com/secu/article.php/3495781

Stevens, A (2007). Backups and the Small Business: Computer Hardware and **Software for Data Backups in Small Businesses**. Personal Computer World, Vol 30 No 12, pp 110-112,
Viewed 05/04/2009, Available at: http://www.emeraldinsight.com/0142-0232/30

Welman, J. C. & Kruger, S. J. (2001), Research Methodology - for the Business and Administrative Sciences, 2. edn, Oxford University Press Southern Africa, Cape Town, South Africa.

Websites

American University of Beirut, http://www.aub.edu.lb/info/data-backup.html

Backup4all, http://www.backup4all.com/knowledge-base.php

Bitpipe.com, http://www.bitpipe.com

Computer Associates, http://ca.com/files/whitepapers/backup_recov_wp.pdf

Searchstorage.com,

http://searchstorage.techtarget.com/sDefinition/0,,sid5_gci214410,00.html

The Linux Documentation Project, http://tldp.org/LDP/sag/html/backup-media.html

The Nairobi Stock Exchange, http://www.nse.co.ke

APPENDICES

APPENDIX I: QUESTIONNARE

A: DEMOGRAPHIC FACTORS

RESPONDENTS PROFILE

1. Title or position of the respondent
   ____
2. No. of Years with the Company
   ____
3. How would you describe your main job role
   ICT Management/administration ( )
   Backup Administration ( )
   Other (Please specify)____

ORGANISATION'S PROFILE

1. Name of organization ____
2. How long has your organization used Computer-Based Information Systems?
   1 to 5 years ( )
   6 to 10 years ( )
   Over 10 years ( )

3. What is the ownership structure?
   Local ( )
   Foreign ( )
   Both Local and Foreign ( )

4. In which of the following categories does your organization fall?
   Agriculture ( )
   Commercial and Services ( )
   Finance and Investment ( )
   Industrial & Allied ( )

5. How many computer users does your organization have?
   1-20 ( )

20-40 ( )
40-60 ( )
Over 60 ( )

6. How many staff are in your ICT department? _______

B: BACKUP STRATEGIES

1. Is critical computer data for your organization identified?
Yes ( )
No ( )

2. Are regular data backups performed?
Yes ( )
No ( )
Others (Please specify)
____

If the answer in 2 above is No, proceed to Section C.

3. Is there a data backup policy in your organization?
Yes ( )
No ( )

4. Are data backup procedures documented for your organization?
Yes ( )
No ( )

5. Who takes responsibility for computer backups in your organization?
ICT personnel ( )
Individual users ( )
Both ICT Personnel and Individual users ( )
Outsourced to third party ( )
Others (Please specify)
____

6. What is the frequency for backing up critical computer data?
Hourly ( )
Daily ( )
Weekly ( )
Monthly ( )
Continuous ( )

Never ( )
Other (Please specify)________________________________

7. What media does your organization backup up to? (Select all that are applicable)
Magnetic Tape ( )
Magnetic disks ( )

8. Are network based backup methods used in your organization?
Yes ( )
No ( )

9. If the answer is (Yes) in 7 above, which methods are employed? (*select all applicable*)
Network Attached Storage (NAS) ( )
Storage Area Networks (SANs) ( )
Web Based Backups ( )

10. Are tests on recoverability of backup data made?
Yes ( )
No ( )

11. If the answer in 10 above is Yes, how frequently are the tests done?
Monthly ( )
Yearly ( )
Irregular ( )
Others (Please specify)
____

12. Are Backup logs maintained?
Yes ( )
No ( )

13. Are unwanted copies of backup media physically destroyed?
Yes ( )
No ( )

C: FACTORS CONSIDERED IN SELECTING BACKUP STRATEGIES

How would you rate the following in influencing the choice of backup strategies adopted?

		Extremely Important	**Very Important**	**Important**	**Somewhat Important**	**Not Important**
1.	Reliability of backup medium					
2.	Ease of use of backup medium					
3.	Volume of data the organization generates					
4.	Capacity of particular backup medium					
5.	Cost of the backup method					
6.	Requirements for data confidentiality					
7.	No of systems' users in the organization					
8.	Computer Network Infrastructure					
9.	Industry and other Regulatory Requirements					
10.	Nature of business					
11.	Frequency of generation of data/transactions					
12.	Data modification times (online versus batch)					
13.	Restoration times associated with particular strategies.					
14.	Extent of centralization of information systems					
15.	Manual versus Automated Backup process					
16.	Impact of systems unavailability to the business					

Please tick in the applicable column.

Are there any other factors that influenced your choice of backup strategy and method?

____

____

D: CHALLENGES TO COMPUTER DATA BACKUPS

How do you rate the following as challenges to a successful backup strategy?

Please tick the applicable column.

		Strongly Agree	**Agree**	**Neither Agree or Disagree**	**Disagree**	**Strongly Disagree**
1.	Volume of data to be backed up					
2.	Requirements for data confidentiality					
3.	Systems downtime while backups are run					
4.	Critical data exists in different locations					
5.	Critical data exists in different formats/operating system environments					
6.	Time taken for backup operations to complete					
7.	Inadequate definition of critical data					
8.	Cost of an effective backup plan					
9.	Backup restoration times					
10.	Inadequate personnel for data backups					
11.	Failure of backup media					
12.	Lack of policy and procedures to support backup procedures					
13.	Poor Electric Power environment					
14.	Lack of top Management Support					
15.	Limited offsite storage options					
16.	User resistance with respect to data in their computers					
17.	Inadequate knowledge and data backup competence of users					
18.	Inadequate time availability for backup tasks					
19.	Lack of clear responsibilities for backup					
20.	Lack of outsourced backup services					

Specify any other challenges you have experienced in relation to data backups

____

APPENDIX II: LIST OF FIRMS LISTED ON THE NAIROBI STOCK EXCHANGE

Firm	**Contacts**
Agriculture	
Rea Vipingo Ltd.	
Sasini Tea & Coffee Ltd.	
Kakuzi Ltd.	
Commercial and Services	
Access Kenya Group	
Marshalls E.A. Ltd.	
Car & General Ltd.	
Hutchings Biemer Ltd.	
Kenya Airways Ltd.	
CMC Holdings Ltd.	
Uchumi Supermarkets Ltd.	
Nation Media Group Ltd.	
TPS (Serena) Ltd.	
ScanGroup Ltd.	
Standard Group Ltd.	
Safaricom Ltd.	
Finance and Investment	
Barclays Bank of Kenya Ltd.	
CFC Stanbic Bank Ltd.	
Housing Finance Company of Kenya Ltd	
Centum Investment Ltd.	
Kenya Commercial Bank Ltd.	
National Bank of Kenya Ltd.	
Pan Africa Insurance Holdings Co. Ltd	
Diamond Trust Bank of Kenya Ltd.	
Jubilee Insurance Co. Ltd	
Standard Chartered Bank Ltd.	
NIC Bank Ltd.	
Equity Bank Ltd.	
The Co-operative Bank of Kenya Ltd.	
Industrial and Allied	
Athi River Mining Ltd.	
BOC Kenya Ltd.	
British American Tobacco Kenya Ltd.	
Carbacid Investments Ltd.	
Olympia Capital Holdings Ltd.	
E.A. Cables Ltd.	

E.A. Breweries Ltd.	
Sameer Africa Ltd.	
Kenya Oil Ltd.	
Mumias Sugar Company Ltd.	
Unga Group Ltd.	
Bamburi Cement Ltd.	
Crown Berger (K) Ltd.	
E.A Portland Cement Co. Ltd.	
Kenya Power & Lighting Co. Ltd.	
Total Kenya Ltd.	
Eveready East Africa Ltd.	
Kengen Ltd	