academicresearchJournals

Vol. 5(8), pp. 229-233, November 2017
DOI: 10.14662/IJALIS2017.037

ISSN: 2360-7858
http://www.academicresearchjournals.org/IJALIS/Index.htm

International Journal of Academic Library and Information Science

Full Length Research

AN ASSESSMENT OF DISASTER RECOVERY PLANNING: A STRATEGY FOR DATA SECURITY

Evans Nyanyu Makwae[1*] and Getrude Nyambeki Nyarige[2*]

[1]Archivist iii Judicial Service commission (JSC) Kenya
E-mail:nyanyuevans@gmail.com/nyanyu2004@yahoo.com, e-mail: evans.makwae@judiciary.go.ke.
[2]Librarian, Kisii University, Kericho campus – Kenya. E-mail:getrudenyarige@gmail.com

Accepted 12 October 2017

The migration from centralized mainframe computers to distributed client/server systems has created a concern on data security. If a disaster occurs to an organization that destroys a server or the entire network, a company may not be able to recover from the loss. Developing an effective disaster recovery plan will help an organization protect them from data loss.

Keywords: Disaster recovery, Data security, Networks

Cite This Article As: Makwae EN, Nyarige GN (2017). AN ASSESSMENT OF DISASTER RECOVERY PLANNING: A STRATEGY FOR DATA SECURITY. Inter. J. Acad. Lib. Info. Sci. 5(8): 229-233

INTRODUCTION

The centralized computer systems are now replaced with or connected to the distributed systems. Also, multiple servers are connected to each other on a corporate network to balance their processing power. If one of the servers in the networked environment crashes, troubles will arise for both the users and the company. There are a variety of reasons that cause systems to crash. For example, the lack of system security and employee sabotage is the main concerns. While computer hackers live outside of the company walls, this is not always the case. Although passwords and firewalls help keep viruses and intruders from entering the corporate systems, sometimes they are useless. Corporate management needs to recognize the necessity for data security. A disaster could cause companies an interruption for a period of time. The Business Recovery Plan is the document used to assist an organization in recovering its business functions. A Disaster Recovery Plan (DRP), however, is a document designed to assist an organization in recovering from data losses and restoring data assets. A DRP should be a pro-active document, a living and breathing document. It does not document the tasks, it is an action plan that is used to identify a set of policies, procedures, and resources that are used to monitor and maintain corporate information technology (IT) before, during, and after the disaster. Possible IT disasters include (Semer, 1998):

- natural disasters, such as fires, earthquakes, lightning, storms, and static electricity;
- software malfunctions;
- hardware or system malfunctions;
- power outages;
- computer viruses;
- man-made threats, such as vandalism, hackers, and sabotage; and
- human error, such as improper computer shutdown, spilling liquids on the computer, and cigarette ash.

Disaster recovery was a term coined by computer vendors between 1960 and 1980 ± the era of the centralized mainframe computer (Colraine, 1998). During that time, a disaster recovery plan was used to backup mainframe computers. A disaster recovery plan was similar to an insurance policy that provided a protection from natural disasters, such as earthquakes, floods, hurricanes, and tornadoes. Disaster recovery plans during these years were typically used by organizations that have large mainframe computers and data sites for daily business operations. Since data recovery planning process was expensive, an alternative was to backup the data from the mainframe computer and store it at alternate locations. During the 1970s, providing backup data services were a lucrative business.

RATIONALE

The purpose of this paper is to assess a disaster recovery planning: a strategy for data security on the basis of empirical evidence. The paper assesses the disaster recovery plans in terms of management involvement and activities, Information Technology involvement and activities, human resource services and possible vulnerabilities. As no extensive research has been conducted in this area in Kenya, the study also fills the gap in disaster recovery planning literature related to this area.

RESEARCH OBJECTIVES

1. To assess management involvement and activities in disaster recovery planning.
2. To analyze Information Technology involvement and activities in disaster recovery planning.
3. To assess human resource services in disaster recovery planning.
4. To identify possible vulnerabilities in disaster recovery planning.

RESEARCH METHODS

The researcher used descriptive survey, of a disaster recovery planning. Description, design and implementation of a disaster recovery planning which provides for long-term data security solutions. However, the researcher contacted the networked server departments in case need were felt to clarify some integrity and also to fill the gap.

LITERATURE REVIEW

Management involvement and activities

Keeping current with IT knowledge

The top-level decision makers may not want to be confronted with computer technology for three reasons. First of all, they may not consider themselves as ``computer people,'' and consequently leave the computer problems to either their subordinates or their IT staff. Second, they may want to learn more about computer technology, but are overwhelmed and confused by all of the literature available in bookstores or in the library. Finally, they may feel intimidated by IT counterparts who know and understand something that they cannot understand. As executives, they may feel intimidated by their lack of understanding and avoid the issue altogether. If, however, they take the initiative to learn how computer technology can help them make better decisions and protect their data, they will become better managers and be able to communicate with their IT counterparts.

Employing qualified professionals to develop and maintain the company's DRP

Individuals who are certified can prove their value and knowledge. Certifications such as the Microsoft Computer Systems Engineer (MCSE) for Windows NT or the Certified Novell Engineer (CNE) for Novell networks are examples. If a company's future plans involve an enterprise network that will include hubs, routers, and bridges, it might also consider employing Cisco trained professionals with Cisco Certified Network Associate (CCNA) or Cisco Certified
Internetwork Engineer (CCIE) certifications. Employing MCSEs, CNEs, and CCIEs to run a company's network also saves time and money on IT training. Similarly, there is training and certification available for disaster recovery. An organization such as the Disaster Recovery Institute offers training and certification on disaster recovery.

Ensuring insurance coverage for LAN

A comprehensive insurance policy may cover data restoration, business interruption, recovery costs, and damage to computer hardware from natural disasters, such as flooding, tornadoes, and earthquakes. Also, a company needs to make sure that they have the proper coverage for all geographical areas.

Organizing specialized response teams to execute the DRP during an emergency

A DRP should be up-to-date and every team member

involved in the recovery process should be familiar with it. The implementation of a DRP should involve specialized teams to be responsible for certain areas of expertise, including initial response team, restoration team, recovery operations team, and logistical support team (Semer, 1998):

- Initial response team. This team is the first set of eyes to evaluate the nature and extent of the damage. These people will determine whether or not business operations can continue on-site or should be moved to an alternate location. If the damage is severe, this team will contact additional response teams for further assistance.
- Restoration team. This team coordinates the damage control, restoration, and reactivation of network resources, which include data files, software, network infrastructure, and communication lines.
- Recovery operations team. If the initial response team determines that operations need to be re-established at an alternate location, the recovery operations team will set up and run the operations at the new location. Their responsibilities include re-establishing the distributed network infrastructures, retrieving backup files, setting up hardware and communication lines, and other related activities.
- Logistical support team. During the transfer of operations to an alternate site, the logistical support team provides logistical support by ensuring that employees can access alternate offices and facilities. They also provide personal support for employees, which includes travel and relocation assistance, cash advances for emergency expenses, crisis counseling, and employee family assistance.

Information technology involvement and activities

Developing a detailed network blueprint

When a disaster destroys most or all of the building, the network will have to be rebuilt. The blueprint of the company's network architecture will allow the IT staff to rebuild the network quickly.

Gaining management's support to the disaster recovery plan

Senior management is recognizing the outcomes of losing corporate data. An effective CIO could understand both IT and management needs, thereby translating the schematics of the technology into management's language.

Monitoring employees' Internet accesses

While the Internet provides the worldwide information at a moment's notice, it also brings with it the threat of sabotage from hackers and viruses. Many of the security concerns regarding the Internet stem from the design of the Internet itself, making it difficult to identify and trace where data are coming from or where they are going (Garfield and McKeown, 1997). Consequently, the best way IT can protect their organization from hackers and viruses is to monitor employees' Internet accesses through firewalls. This will greatly reduce the dangers from hackers outside the company.

Standardizing hardware and software

Any organization having heterogeneous hardware and software will create difficulties of rebuilding the network. For example, if some departments are using Macintosh computers while others are using PCs, the rebuilding process will take even longer. Therefore, having a homogeneous enterprise system can reduce the complexity of rebuilding the network.

Securing support from IT vendors

Implementing a DRP needs to secure support from both routine vendors and specialized vendors. Routine vendors are suppliers who provide daily services, such as hardware and software support, e-commerce support, and telecommunications service. Specialized vendors are companies that provide specific disaster recovery services. Their services include data salvage and restoration, alternate office space, alternate backup sites, and emergent lease of hardware and equipment.

Performing routine backups

A backup procedure should be performed in order to ensure that all mission-critical systems are stored on LAN servers instead of users' workstations, floppy disks, or ZIP disks and flash disks which are not subject to system backups. This ensures that the data are centrally located in one place to facilitate backup and recovery procedures.

Ensuring smooth interface between client/server and mainframe systems

Interface applications that allow data to be exchanged between mainframe and networks will need to be identified and included in the backup and recovery procedures. Any failure of backing up these applications may complicate the recovery process and the integrity of data and system.

Using redundant array of independent disks (RAID) technology to capture on-line transaction activity

RAID provides mirrored copies of data on multiple disk drives that create up-to-date copies of data files. RAID also provides capability of fault tolerance, providing accessibility to data in the event of a partial disk failure.

Preventing LAN from viruses' attack

Choosing the right anti-virus software for the LAN is imperative for protecting the data.
After selecting suitable programs, system administrators should make regular sweeps of the LAN to ensure system integrity at all times.

Protecting hardware from environmental damage

Make sure that surge protector and antistatic mats are installed on all LAN servers in order to protect them from static electricity. According to a report, computer users in the Midwest and North Central USA suffer the most data loss due to static electricity during the winter dry air (Sutton, 1998).

Connecting uninterruptable power supplies (UPS) to key servers and equipment

The power-related problem is one of the major causes of losing data. If a server suddenly loses its power, there is a chance that the data on the hard drive will be lost. By installing UPS and/or a backup power supply on the entire LAN servers could maintain the integrity of the data on the server.

Identifying possible vulnerabilities

Monitoring the vulnerability will prevent a problem before it occurs. For the most companies, the main areas of vulnerability may include (Rothstein, 1998):

- backup storage locations for data;
- security;
- physical security;
- the room or building that is housing the computers,
- electrical power;
- fire detection and suppression;
- depending upon one person for information;
- management controls; and
- reliability of telecommunication services.

Other areas of vulnerability include employee resignation, repairing a roof leak in the computer room, computer virus infection, and so on.

RESULTS AND DISCUSSION

According to the third annual information security survey conducted by Information Week and Ernst & Young, nearly half of the more than 1,290 respondents representing information systems chiefs and security managers suffered security-related financial losses in the past two years (Panettieri, 1995).

Most companies hesitate to develop a disaster recovery plan until a disaster occurs. According to another survey (Patrowicz, 1998), 85 per cent of the Fortune 1,000 companies have disaster recovery plans (Table 1). Within these companies which have disaster recovery plans: 80 per cent have plans that protect their data center resources; 50 per cent have plans that protect their networks; and less than 35 cent have plans that protect their data on PC LANs.

In an Ernst & Young/Computerworld Global Information Security Survey of 4,255 IT and information security managers, 84 per cent of them said that their senior management believes that security management is ``important'' or ``extremely important.'' Of these respondents, over 50 per cent of them stated that they lack a disaster recovery plan (Anthes, 1998). However, most of the problems stem from the lack of communication at the corporate level. The growth of distributed systems and the global business environment make corporate decision makers believe that having a backup or recovery plan is necessary. Many companies need to process the mission critical information stored in distributed or client/server systems throughout entire enterprise networks. One of the success factors for a company's business operations is based on the continuance of these enterprise networks. Client/server systems have replaced the centrally located mainframe, residing at multiple sites in a building or across a corporate WAN.

Consequently, protecting these client/server systems has become a major priority for corporations today (Colraine, 1998). Distributed systems are becoming an architectural standard for networked organizations. These systems have diffused mission-critical data across local area networks which extend corporate resources to remote work sites. As distributed systems continue to replace the ``glass house'' environment of the mainframe, the data decentralization is going to increase in the future (Mello, 1996).

According to a survey conducted by the research group of David Michaelson & Associates, the respondents stated that 43 per cent of the data housed on corporate PC LANs today is mission related (Mello, 1996). Of these respondents, 77 per cent employ a continuous or daily backup for their PC LANs, and 89 per cent of them follow some kinds of backup procedures. It is a dramatic increase from a similar 1993 survey, in which only 45 per cent of the organizations stated that they backed up their

Table 1. company with disaster recovery plans

Data Recovery plan (DRP)	Percentage
Data center resources	80
Networks	50
Data on PC LANs	35

PC LANs on a continuous or daily basis. As the distributed system model continues to become the de facto standard in most corporate networks today, companies will eventually learn ± either by proper planning or their own unfortunate experience ± that having a disaster recovery plan is vital for their survival in today's networked environment.

CONCLUSION

A disaster causes an event that halts the critical business functions within an organization. It can be as simple as a power disruption to a data server or as serious as a threat to the entire building. Disaster recovery is the process of correcting the problem and getting the critical business functions back online. A disaster recovery plan is, therefore, a predetermined set of instructions that describes the process of disaster recovery.

Developing a DRP needs some hard work such as planning, brainstorming, and cooperation from both corporate management and employees. The plan can be as simple as describing how to back up a server, or as complicated as describing what to do after a hurricane destroys the building. The main source of developing a DRP is to understand the particular needs of the organization.

There are advantages and costs of having a DRP. Some of the advantages are the reduction in data loss, minimizing the need of decision-making process during a disaster, and the protection of company employees. It also causes extra expenses and requires manpower. Despite the questions that arise when considering a DRP, companies should focus on the most important commodity: company data. Depending on the importance of the data, developing a DRP can be more economical than replacing the lost data.

As corporations become increasingly dependent on computers and the Internet for their daily activities, the data generated from their work are becoming critical. Companies that rely on their computer systems and networks to do their business can suddenly lose everything if their computer systems go off-line or are corrupted by a virus. In this electronic age where computers are enhancing the talents and skills of people, the data are now filling the seats of executive boardrooms and corporate offices. At one moment in our country's history, the battle cry used to be ``survival of the fittest.'' Today, as computer technology and data are becoming the important commodities of the future millennium, the new battle cry is ``survival of the data.'' Consequently, data are protected from corruption and it is one of the major functions of top-level management and IT professionals today.

REFERENCES

Anthes, G.H. (1998), ``Lots talk, little walk'', Computerworld, Vol. 32 No. 38, pp. 70-1.

Colraine, R. (1998), ``Protect more, recover faster is the rule'', Computing Canada, Vol. 24No. 30, p. 35.

Garfield, M.J. and McKeown, P.G. (1997), ``Planning for Internet security'', Information Systems Management, Vol. 14 No. 1, pp. 41-6.

Jackson, J. (1997), ``Give your LAN a hand'', Security Management, Vol. 41 No. 8, pp. 44-52.

Leary, M.F. (1998), ``A resource plan for your LAN'', Security Management, Vol. 42 No. 3,pp. 53-60.

Mello, J.P. Jr (1996), ``Taking a crack at backup'', Software Magazine, Vol. 16 No. 10, pp. 85-8.

Panettieri, J.C. (1995), ``Security'', Information Week, 27 November, pp. 32-40.

Patrowicz, L.J. (1998), at http://www.cio.com/ archive/040198_disaster_content.html

Rothstein, P.J. (1998), ``Disaster recovery in the line of fire'', Managing Office Technology,Vol. 43 No. 4, pp. 26-30.

Semer, L.J. (1998), ``Disaster recovery planning for the distributed environment'', Internal Auditor, Vol. 55 No. 6,pp.41-7.

Stefanac, R. (1998), ``When it comes to disaster, it's pay now or later'', Computing Canada, Vol. 24 No. 30, p. 35.

Sutton, G. (1998), ``Backing up onsite or online: smart ways to protect your PC from disaster'', Computer Technology Review, Vol. 18 No. 2,