Disaster Recovery Planning for Data Centers and IT Services

Yasin Akıllı[1], Ali Güneş[2]

Istanbul Aydın University, Istanbul [1, 2]

Abstract: In accordance with the technological developments in today's world many companies implement their vital operations on their data centers and IT services.In connection with the fast development in technology and risimg complexity of business processes, the control of the systems and critical data that companies have, became more and more complicated. Therefore; it became an obligation for most companies to have a well-organized "Disaster Recovery Plan".

Keywords: Disaster Recovery, Business Continuity, Disaster Recovery Plan, Disaster Management.

1. INTRODUCTION

Today, together with the developments in Information and Communication Technologies, companies make investment on their IT services and data centers to provide fast and continuous services to their users and customers. They set up these data centers with the systems presenting the best services, the highest accessibility and again for these systems in order not to face with access problems there is an increasing investment for all IT structure.

Companies need a well-arranged Disaster Recovery Plan for the continuity of their data centers, server systems and IT services to be able to manage the disaster recovery period effectively and to cut through the disaster with minimum data and economical loss; because in an emergency disaster situation they may lose access to some part of the system or all IT and server systems may be out of order.

This article provides a guideline in planning IT processes showing up to date Disaster Recovery solutions, strategies and suggestions for an unexpected disaster situation to cope with the losses, discontinuities in data centers and IT services.

2. BUSINESS CONTINUITY PLAN

Companies all over the world to be able to guarantee the business continuity became more and more dependent on IT industry. In an unexpected disaster situation, the systems that are directly depending on IT infrastructure, need high-level, intense studies; accordingly, it can be said that planning processes of business continuity directly effects all business processes.

Business continuity plan, includes the occupations and processes that the company will prompt in a disaster situation.

It includes the studies that will be carried out in an emergency situation to prevent the the possible damage on critical services and it aims to get over the crisis with a minimum loss and damage [1].

Disaster recovery plan, on the other hand, includes planning, development, and evaluation studies and it provides the efficient and effective continuation of bussiness functions.

Main processes in an extensive Disaster Recovery plan are listed below:
- Identification of critical applications
- Data and system procedures
- Data and system recovery procedures
- Maintenance and evaluation of procedures
- Identification of installation support vendor for IT infrastruce and system needs and to do necessary agreements (Identification of your solution vendor)

3. DISASTER RECOVERY PLANNING

Today, either for big or small companies it is a great need to have a disaster recovery plan. This plan needs to be as extensive as possible and it should provide the continuity of bussiness processes eliciting the starting of other critical processes within the shortest possible time. Besides, this plan must foreseen the storage and restoring of all data backups avoiding data losses [2].

3.1.   Preliminary And Planning Stages
Instead of using a ready Disaster Recovery Plan, created for a special company, companies need to do analysis and choose the best fit disaster recovery processes and solutions for their own structures and prepare their own recovery plans. By the way; this will both create a better recovery management strategy for IT managers and the company will gain more benefits.

To prepare an IT Disaster Recovery Plan, only special for your company, and to have an extensive, effective, and a well-arranged IT Disaster Recovery Plan, you should follow the stages given throughly:

- Identification of Disaster Recovery management plan objectives and scope,

- Documentation of data center, server systems, hardware and software structures,
- Conducting of bussiness-impact analysis for server systems and IT services,
- To designate RTO and RPO assets for server systems and IT services,
- Immobilization of Disaster Recovery solutions consistent with the company's infrastructure,
- Specification of Disaster Recovery operation teams and their responsibilities,
- Noting critical server systems and operation recovery priorities,
- Identification of probable disaster scenerios and deduction problems,
- Creating the list of employers for disaster recovery management and operations,
- Provision of a forecast budget proposal for DR solutions and processes,
- Preparation of Disaster Recovery center, communication links and location maps,
- Identification of vendors and technical support companies,
- Testing of Disaster Recovery Plan periodically.

3.2. Protection Stage Of Data Center And IT Assets
Within the DRP phase, to protect data center and IT services in an unexpected disaster situation to prevent losses and unaccessibilities, the steps given below should be followed:

- Immobilize your most critical applications and data: Companies need to decide which applications and data are most valuable for them, which ones are most critical and which data is valid for their customers, such as; internal accounts, financing etc.
- Virtualize your critical systems and applications: This is not only reduce your work intensity and costs but also make your environment more suitable for disaster recovery. Virtual environments are more useful and more easy to move. Virtualization; protecting individual components and animated parts, will diminish the complexity and will make recovery stages easy to manage [3].
- Immobilize your RPO(Recovery Point Objective) and RTO(Recovey Time Objective) values realistically: It should be decided before if which data can be lost, how long and when will the critical applications be online again after a disaster. Be sure that your objectives are realistic, attainable, and accurate.
- Create your data backup and recovery procedures:

Decide your failover(a secondary system that takes the control in a disaster situation) and failback(recovering system and services back after a disaster)times and the conclusion will show you your protection level, your recovery speed and your expected costs.

- Keep your data and system backups up to date: In Disaster Recovery Center, data backup systems and in storage systems; backup your data frequently, by the way, in an unforeseen disaster stiuation you will have less data loss. Besides, you will meet your RTO assets with less effort.
- Automate your bussiness and operation processes: Don't let human errors cut your way! If you do your automatical disaster plans thanks to the suitable automation, your disaster recovery will take minutes rather than weeks. This system eliminates many of the management problems for system users. Since network and virtual machine configurations have been made before, some processes like restarting of applicaiton can be done automatically.
- Plan your risk management accurately: Many lack of access problems faced in IT services are not called as a disaster; otherwise; they are caused by some faults in procedures. Prapare your procedures on how to update and upgrade the services and IT systems before the operations, then do your operations depending on these procedures.
- Give responsibilities: Give personal responsibilities for everyone in your team, be sure that each personal is ready to move and work in any critical situation.
- Prepare your Failback plan after a disaster: An experienced disaster and a disaster recovery made up can not create a whole disaster recovery plan. You need to plan your failback stages to reverse original operations of the systems after the disaster is over [4].
- Choose your solution partner: Agree wtih a firm that will support give technical assistance with your IT infrastracture and server systems. In an emergency stiuation, they will help you to recover quickly and manage the crisis situations.

3.3. Classification of the Disaster
Identification of the risk that your company may face, is the major and the most important part of being ready for a disaster.
In the list given you can find some basic IT problems that interrupts or prevents operations. Apart from these, other risk types can be classified as; intentioanal actions, infrastructure problem and environmetal disasters.
Nearly all componies in the world ,if not all, face with any one of these problems. Disaster types are listed in Table-1.

Table -1 Disaster Types

Disaster Types			
A	**B**	**C**	**D**
Hardware Errors	Computer Viruses	Electricity Outages	Fires
Software Errors	Hackers	Air conditioning malfunctions	Flood of
Network Errors	Internet Outages	Power Supply Failures	Earthquakes
Data Corruptions	Test and update process errors	Wiring faults	Terrorist Attacks

Your Disaster Recovery Plan must be qualified enough to make your all system and data operating again within the shortest possible time in any natural disaster or technical disaster situation.

3.4. Disaster Recovery Plan Tiers

Disaster Recovery Plan for data centers and IT services can be examined in 4 tiers according to their stages and strategies they use. These tiers are featured in rhe Table-2 below:

Table-2 DR Plan Tiers

Disaster Recovery Plan Tiers	
Tier Level	**Data Protected Methods**
Tier 0:	None DR Plan - None Data Backup
Tier 1:	DR Plan + Offsite Data Storage + Backup
Tier 2:	Tier 1 + Redundat IT Systems
Tier 3:	Tier 2 + Passive Disaster Site
Tier 4:	Tier 3 + Redundat Active Data Center

Tier 0: It defines data centers with one site and they donot need any Disaster Recovery processes since in this tier there isnot any recorded data or documentation belong to the company so consequently there is no risk of emergency for the companies in this stage.

Tier 1: Companies that have IT services and data centers in this step, have a Disaster Recovery Plan and save and manage their data in an off-site storage site along with the main data center.

Tier 2: This tier encloses all features of prior tier and besides all, for the IT services that serve for critical processes in data center, they host a reserve system, hardware and infrastructure resources that can be used in an emergency situations.

Tier 3: Companies that have IT services and data centers in this tier have all features of tier 2 and add to these they

There are some standarts for the data centers that have a first rate importance for IT information industry. Among all these the most widely- accepted ones are TIER certifications. These certificates given by 'uptime institute' that evaluate data centers for their maintenance, management and design areas. After the evaluation, companies that have the announced values and assets are entitled to a TIER certification [5].

have a secondary data center to which they continually transfer critical data.

Tier 4: Tier 4 encompasses all the features of Tier3 and in addition, , for the IT services and critical data that serve for critical bussiness processes,they have a second data center with the same qualities of the main site. Therefore; some backup and migration processes are done in both of these centers.

3.5. Bussiness-Impact Analysis

Within the formation stage of Disaster Recovery Plan for data centers and IT services, one of the most important steps is to make a disaster bussiness-impact analysis which includes the studies that show the foreseen negative effects of the disaster before it happens.
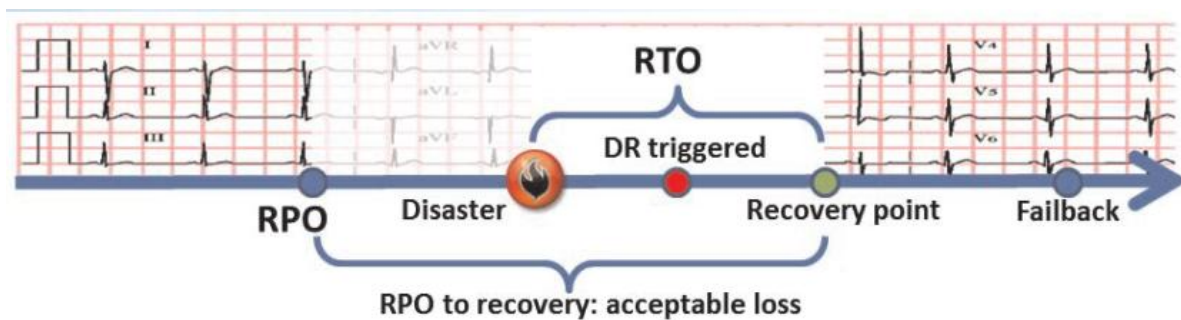

Figure 1. RTO and RPO

While creating a Disaster Recovery Plan, RTO and RPO considered as an important criteria and requires an accurate planning.

Recovery Time Objective: It is the guessed elapsed time that passes till all the processes come back to operating conditions again. The aim is that this time must be shorter than accepted lack of accessibility time [6].

Recovery Point Objective: It is the range of the data loss between the time that processes are interrupted and restarted again. (Figure 1)

For your company's data center and for all critical services:

- Define your RTO and RPO values,
- Impact analysis on business processes should be done,

- These listed should be added on Disaster Recovery Plan,
- The most effective and fast recovery solutions should be determined,
- Qualified recovery team should be organized,
- Necessary education should be given to the responsable recovery team.

When the steps listed above are done completely , in an unexpected natural disaster, you could verify permanance of IT services and server systems with minimum data less abd lack of access [7].

3.6. DR Teams and Responsıbilities

Another importatnt step in creating Disaster Recovery Plan is to designate Disaster Recovery management and operation teams to take over the control of crisis management actively in an unexpected crisis situation in which all server systems and critical bussiness services will be damaged.

While preparing a Disaster Recovery Plan organizing teams for management and opertions has a avital importance for the activation of the Disaster Recovery Plan. For this reason before a real disaster situation happens, the responsible people who will manage and operate the systems need to be specified and listed with their contact information.(Table 3)

Table-3 DR Management Team

Disaster Recovery Management Team			
Name	**Title**	**Emergency Phone**	**Disaster Recovery Role**
Person A.	Head of IT	01 000 xxx	Team Lead
Person B.	System Expert	01 000 xxx	Coordinator of Recovery Team
Person C.	System Engineer	01 000 xxx	Server Systems Responsible
Person D.	Netwrok Specialist	01 000 xxx	Network Systems Responsible
Person X.	Storage Admin	01 000 xxx	Data Storage Systems Responsible
Person X.	Backup Amin	01 000 xxx	Data Backup Systems Responsible
Person X.	Security Amin	01 000 xxx	Security Systems Responsible

3.7. Disaster Recovery Solutions

Throughout the creating process of bussiness continuity and Disaster Recovery planning,it is crucial step to choose the best solution conforming with the economical and technical structure of the company.

While choosing a Disaster Recovery solution best fit with the data center and IT system architecture of the company,both the disasters that will come out of environmental reasonss and the ones caused by technological problems should be taken into consideration. As now, the most extensive Disaster Recovery solutions for data centers and IT systems presented by information technologies and the best ones generally accepted by IT managers are listed below:

- Clustering
- Replication & Mirror
- Backup
- Cloud Computing
- Disaster Recovery Site

If all the solutions listed above are planned after a fair business impact analysis, in an event of a disaster the company will be moved to the operatig conditions again without any data loss and access problems [8].

4. BENEFITS OF DISASTER RECOVERY PLAN

A well organized and accurately choosen Disaster Recovery Plan will supply many adventages for the companies;

- It provides to forestall the possible risks on IT services and data center or at least for the disasters that cannot be stopped it reduces the possible damages,
- It reduces and prevents possible economical losses,
- It prevents loss of status for the company,
- It supplies the successful recovery of business operations and functions,
- It diminishes the damage on the vital functions in a disaster,
- It reduces operation damages ,
- It raises the stability of the company,
- It helps to define the critical and precision systems,
- It reduces the time spent for disaster alert decision and it provides a foreseen planned recovery processes,
- It prevents the confusion and complexities in crisis situation and also the human errors caused by over-stress,
- It protects company's assets and studies,
- It provides a good teaching and exercising material for the new starters.

5. CONCLUSION AND SUGGESSTIONS

In today's world with the developments on information and communucation technologies and companies' expanding demand for data centers and IT systems, to be able to guarantee the bussiness continuity Disaster Recovery Plan became the most important building block of IT systems.

Disaster Recovery Management, on the other hand, is no more a choice but an obligation for the companies that lay their services before their employers and customers from these data centers and IT systems.

Disaster Recovery Plan; once more, has a vital importance for the services serving from data centers and IT systems in an event of an unexpected disaster since it provides the correct management of the processes and recovery of the services with minimum data loss and distruption.

REFERENCES

[1] Bilişim Derneği, Türkiye. Kamu-Bib İş Sürekliliği Çalışma Grubu. Türkiye Bilişim Derneği. [Çevrimiçi] 2016. http://www.tbd.org.tr/usr_img/cd/kamubib17/AnaMenu.htm.

[2] Felaketten Kurtarma ve Depolama. Doğdu, Erdoğan ve Nihat, Yurt. Ankara : Türkiye Bilişim Derneği, 2009. Türkiye Bilişim Derneği, Kamu Bilişim Platformu XI Final Raporu. s. 21-36.

[3] Menken, Ivanka. Virtualization The Complete Cornerstone Guide to Virtualization Best Practices. basım yeri bilinmiyor : Emereo Pty Ltd., 2010.

[4] Buyya, Rajkumar ve Broberg, James. Cloud Computing: Principles and Paradigms. New Jersey : John Wiley & Sons Inc., 2011.

[5] Itadvisor. Tier 3 Veri Merkezi Standartlarını Belirliyor. itadvisor.com. [Çevrimiçi] 2012. http://itadvisor.com.tr/tier-3-veri-merkezinde-standartlari-belirliyor/.

[6] Dinç, Erdal. RTO ve RPO Nedir? Erdal Dinç Kişisel Web Sayfası. [Çevrimiçi] 2014. http://www.erdaldinc.com/recovery-point-objectiverpo-ve-recovery-time-objectiverto-nedir/.

[7] Akpınar, Haldun. Prof. Dr. Haldun Akpınar. Enformasyon Teknolojisi ve İşletmecilik Öğretimine Etkileri. [Çevrimiçi] 2015. http://haldunakpinar.com/yayinlar.htm.

[8] Çözümpark, Bilişim Topluluğu. Storage üniteleri arasında data mirror. Çözümpark. [Çevrimiçi] 2015. https://www.cozumpark.com/blogs/default.aspx.

BIOGRAPHIES

Yasin Akıllı, is still working as a System Virtualization Admin in Avea Iletisim A.S. , he has been carrying on studies about Backup and Storage Administration and Disaster Recovery. He has been working on ITindustry as a System Engineer for about 10 years. He has completed Microsoft System Engineer certifications and got the title of MCITP. He has a Master's Degree in Computer Engineering at Istanbul Aydın University.

Prof. Dr. Ali Güneş is a professor of Computer Engineering Department of Istanbul Aydin University. He is also the Head of Distance Education Research and Application Center at Istanbul Aydin University. He currently teaches, consults and conducts research on computer software development, application of information technologies and new learning technologies in computer education. His minor is distance education and e-learning. He has been studying computer software development, integrated education and technological developments on education for more than 30 years in the academic field.