UNIVERSITAS UTPADAKA SWASTIKA
Jl. KS Tubun No.11 Tangerang 15112 Banten, Telp. (021) 5589161-62 Fax. (021) 5589163
JISI Jurnal Ilmiah Sistem Informasi
ISSN: 3046-711X

Implementation of Disaster Recovery Planning in Call Center System

Fajar Muttaqi

Utpadaka Swastika University, Tangerang, Indonesia, 15112
E-mail: fajar.muttaqi@utpas.ac.id

Accepted: March 26, 2024 | Published: April 30, 2024

ABSTRACT

Call center management refers to how leaders manage the center and includes activities such as forecasting, scheduling, queue management, agent training and coaching, and, of course, ensuring customer contacts are handled professionally and efficiently. Call Center services in Indonesia do not reach the public. To achieve this, a call center is used for business services. To reach the target, effective call center performance is needed by the call center system appropriately. DRP is one of the solutions to reduce the data risk, because of disasters and other threats so the system has another backup.

KEYWORDS: Component, Data Center Disaster, Data Backup, Business Continuity

1. Introduction

As organizations progress into a technological environment, the amount of data stored digitally increases dramatically. This data is sensitive to the organization to do its job and can hinder the operation of the organization if something happens to the data. A study in 2014, revealed that 20% of companies that experienced data loss cost them between $50.000 and $5 million [1].

Disaster Recovery Planning (DRP) [3, 4] is associated with the recovery of a key set of IT systems and infrastructure components. The Business Continuity planning [2, 3, 4, 5] is related to the enterprise as a whole piece dealing with business processes. So, Disaster Recovery (DR) thoughts are part of the Business Continuity (BC) [5;6]. From the IT perspective recovery will usually stand for establishing support for the processing and communications functions considered crucial by the business society and then establishing support for subsidiary systems. From the business perspective recovery will mean, being able to execute the business functions that are at the center of the business and then being able to execute subsidiary functions. Issues that may affect Business Continuity must be documented and addressed as part of the DR endeavor, even if the only action taken is to postpone them to the BCP team or to bring them together as input to a future BCP effort if this is a separate DR project [5;6].

PT JKL is an insurance company that was founded on 27 November 2014. PT JKL has 1.400.000 insured as of 2014.
PT JKL both have 1 centralized data center and 1 Disaster Recovery Center Server (DRC Server). A problem that often happened in the past few years that makes the system unusable such as power failure, and damaged devices. The above problem causes:

a. The system availability level is not good, causing SLA (Service Level Agreement) at PT. JKL not fulfilled.
b. The 24-hour service to the community stalled to gain complaints from the public.
c. Revenue PT. JKL is reduced.

According to a survey completed in 2014, human error is responsible for 40% of all data loss, as compared to just 29% for hardware or system failures. An earlier IBM study determined data loss due to human error was as high as 80%, so we know it's somewhere in that range [2].

Disasters such as floods, hurricanes, fires, earthquakes, and many disasters can happen. It has an impact with infrastructure, especially servers, and storage. The source of the threat consists of several things as follows:

1) Natural disasters such as floods, forest fires, hurricanes.
2) Failure of infrastructure and technology, such as power failure, data corruption, virus network, software corruption, and hardware failure.
3) Human failures such as poor training or inadequate supervision, because of human error, bad procedures, or improper implementation of procedures.
4) Criminal activities such as burglary, hackers, and insiders.

DRC is a solution to reduce the data risk, so PT JKL has another backup server that supports the production server.

2. Literature Review

2.1 Disasters

Disasters can be interpreted as events extraordinary, sudden and unplanned ones can cause damage and loss. Disasters are grouped into 3 types. the first type is a natural disaster that is a disaster that occurs due to natural processes such as earthquakes, typhoons, etc. human disaster is a disaster that occurs due to human negligence factors such as operator error, piracy, the spread of viruses, etc. and Finally, environmental disasters, those that occur due to environmental factors such as software system errors, damage to communication networks, etc. [7]. In a business environment, disasters can be defined as disruptions to critical applications and data that occur widely due to failure of computing processes and network disruptions. So that an organization is unable to carry out business functions in a certain time [7].

Disasters are also interpreted as sudden events that cause a lot of damage, such as fires, storms, or very bad accidents. Disasters are events or series of events that threaten and disrupt people's lives and livelihoods caused by natural, non-natural, or human factors. So disasters result in human casualties, environmental damage, property losses, and psychological impacts.

2.2 Disaster Recovery Plan

Disaster Recovery Plan (DRP) is one of NIST's version of contingency plans which includes organization preparation and response when a disaster occurs. If seen from the name,
In the industrial world, DRP is often focused on information technology and is designed to restore the operation of the target system, application, or computer facility to the location alternative after an emergency.

DRP is a document that defines each activity, action as well procedure that must be carried out by all stakeholders involved to save assets (in this case it is IT services) in the technology sector information. DRP is usually described in
set of policies and procedures for use in preparing for recovery or keeping up sustainability of information technology services which is critical for the organization after a disaster happens.
DRP simply can be defined as an action plan document (response plan) to disaster events. However, in its preparation, DRP requires several processes such as recording all assets (IT services) owned by an organization, recording negative risks that could potentially be a disaster for the organization, and business impact analysis (Business Impact Analysis - BIA) as consideration of decisions in the DRP. The ability of the infrastructure to resume operations as soon as possible during a significant disruption such as a major disaster that cannot be predicted in advance.

2.3 Data Center

Data centers are simply centralized locations where computing and networking equipment is concentrated to collect, store, process, distribute, or allow access to large amounts of data. They have existed in one

form or another since the advent of computers [8].

Because of high concentrations of servers, often stacked in racks that are placed in rows, data centers are sometimes referred to as server farms. They provide important services such as data storage, backup and recovery, data management, and networking. These centers can store and serve up Web sites, run e-mail and instant messaging (IM) services, provide cloud storage and applications, enable e-commerce transactions, power online gaming communities, and do a host of other things that require the wholesale crunching of zeroes and ones [8].

3. Method

This research uses a qualitative approach to this type of study case, namely examining a case that occurs at a certain place and time and looking for contextual settings for the case, by collecting material from many sources and clear information to get a detailed case description. This research is a research that is Juridical empirical because of this research focuses on researching the field thoroughly, systematically, and accurately and supported by library research and data secondary that is already available previously. The results of this study are analytical descriptive because this study is expected to get a picture thoroughly regarding the implementation of disaster recovery and contingency planning in the protection of vital archives at PT JKL.

4. Results

PT JKL has 4 users with 1 router, 1 production server, and 1 DRC server. The users input data to systems in the production server and DRC server. When the production server has a problem, the users can access to DRC server. Both servers have the same data. When the production data is down and being repaired, the server will be switched to the DRC server. After the production server has been repaired, it will sync the data between the production server and the DRC server. After finishing the sync process, the server would switch to the production server. This process would make the operational system run without hindering any workflow.

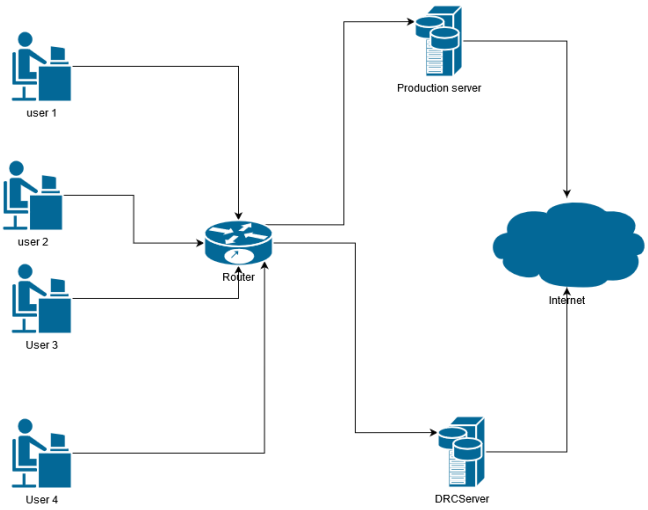

Figure 1. Application and Database Diagram Existing

DRP needs to analyze and identify possible risks in a process that can be anticipated by drawing up an emergency plan to handle problems that arise due to these risks. Therefore, to understand this concept it is necessary to understand in advance about disasters. The disaster itself is defined as serious damage that happened to many people, materials or the environment encouraging the ability of the parties affected by the disaster to handle it using its own resources. In this study, it is certainly a disaster devoted to material damage as intended because the material is a vital archive in an organization.

As for the PT JKL itself, awareness about the identification of a disaster may be still not visible, in general, BPN is more attentive to disasters caused by human activity So effort protection is still limited to CCTV and lack of operation, the spread of virus. This is possible because until now the risks are often experienced only in limited tucked archives or lost. While cases like neither flood nor fire were experienced. From the point of view of the DRCP paradigm of course this is not good, the organization must understand what might

be a risk/disaster. Planning for management disaster starts from asset identification that the organization has. Some vital assets owned by organizations such as:

1. Computer
2. Electronic Archive
3. Non-electronic Archive
4. Data Server
5. Human Resource

Looking at cases that occurred at PT JKL, it seems like planning needs to be done mature risk management from a government agency, including through 3 stages, namely:

1. Pre-disaster stages

In this stage, the most important is identifying any archive that needs to be saved in times of disaster, both electronic archives or physical. For physical archives building design needs to be considered like more storage space position both close to the mitigation pathway disaster. Storage using a roll pack rated is enough for security from the danger of fire or water, though this needs to be media to keep the archive stored in digital form. Every government must have a support server, so if the main server has a virus, then data backup can be done. Tool fire extinguishers and lane disaster mitigation must also be installed inside the building. The most important is to do socializers and simulations if a disaster occurs to employees so employees have no panic and confusion when facing disaster.

2. Stages during a disaster

In this stage, things are necessary to run an SOP disaster mitigation. The SOP must be arranged beforehand if a committee can be formed for disaster management. HR usually will panic and forget about organizational assets, of course, this is a natural thing, however, it needs to be established each other's responsibilities employee at the time of the action rescue, for example, flooding happens, anyone who has to build to save assets, or when a fire breaks out, the employee turned on the water sensor so that the pipe drains the water in a way automatically, while the employee saves themself.

3. Stages after a disaster

In this stage, the main focus is recovery, this is usually done by identifying any assets that can still be saved, the physical archive separated by category of the damage, and the next rescue process. While electronic archives can move to a new server or trace back the damage already to what extent.

Therefore, in order to be effective the organization must prepare a plan for disaster recovery consisting of:

1. Organizational philosophy, vision, mission, and goals related to election and continuation plan effort
2. Appointment of the Executive Committee Disaster Management to take action in a situation absence of a Board of Directors
3. Clear directions and the scope of disaster recovery based on risk assessment
4. Tasks, authority, and responsibility of each employee to manage conditions critical
5. Organizational recovery plan for each branch, department, facility, and function within the institution
6. Equipment for preparation of conditions disaster emergency
7. Training program that is comprehensive for all employees carried out in a certain interval of at least a year once. Training can contain material about identification and equipment usage, mapping disaster areas, basic first aid and technique survival, and explanations regarding the responsibilities of each in a disaster situation.
8. A written copy of the plan for the final disaster recovery that is distributed to each branch and department heads

5. Conclusion

Implementation of the DRC system at PT. JKL is the backup server (DRC) that will automatically work, so the production server is still in uptime status and avoids downtime. Disasters such as floods, hurricanes, fires, earthquakes, and many other disasters can happen. It has an impact on infrastructure, especially servers and storage. DRC is a solution to reduce the data risk.

In the pre-disaster stages the most important is identifying any archive that needs to be saved in times of disaster, both electronic archives or physical. For physical archives building design needs to be considered like more storage space position both close to the mitigation pathway disaster. In stages during a disaster, the thing is necessary to do is run an SOP disaster mitigation. The SOP must be arranged beforehand if a committee can be formed for disaster management.

HR usually will panic and forget about organizational assets, of course, this is a natural thing, however, it needs to be established each other's responsibilities employee at the time of the action rescue, for example, if flooding happens, anyone who has to build to save assets, or when a fire breaks out, the employee turned on the water sensor so that the pipe drains the water in a way automatically, while the employee saves thyself. In this stage, the main focus is recovery, this is usually done by identifying any assets that can still be saved, the physical archive separated by category of the damage, and the next rescue process. While electronic archives can move to a new server or trace back the damage already to what extent.

References

[1] The Disaster Recovery Preparedness Council. The State of Global Recovery Preparedness Annual Report, 2014.
[2] Snedaker, Susan & Rima, Chris. (2014). Business Continuity and Disaster Recovery Planning for IT Professionals. Waltham : Syngress.
[3] Jon William Toigo (2003): Disaster Recovery Planning: Preparing for the Unthinkable (3rd Edition): Harlow, UK: Prentice Hall.
[4] Susan Snedaker (2007): Business Continuity and Disaster Recovery Planning for IT Professionals, Syngress Publishing.
[5] BCI Business Continuity Institute (2007): "Good Practice Guidelines 2007, A Management Guide to Implementing Global Good Practice in Business Continuity Management."
[6] Kibildis, George W. (2005): Business continuity planning in the real world, Disaster Recovery Journal, vol.18 (3).
[7] Gregory, P. 2008. IT Disaster Recovery Planning for Dummies. Indiana: Wiley Publishing, Inc.s
[8] Geng, Hwaiyu. 2014. Data Center Handbook. Wiley Publishing.