Network Disaster Recovery Plan

Name

Institutional Affiliation

Network Disaster Recovery Plan

**Introduction**

Business continuity planning and disaster recovery planning are the most critical elements of business, which are often ignored. Business must consider developing a well-structured disaster recovery plan and prepare associated documentation that not only encompasses disaster recovery, but also business continuity. Disaster especially in network and information system can be short term or long term, but with the organization readiness it becomes easier and ready for any adversity (Zhang et al., 2020). This paper will clearly provide an overview of network disaster recovery plan, which will also entail the components of each plan by providing an overview that must be followed by an organization, to make better disaster recovery.

A network disaster recovery plan involves a set of methods designed to prepare a company to respond to interruption of network services during a natural catastrophe. These network services ensure there is no interruption of internal and external communication and data sharing within the company. It covers plans and procedures of local area network (LAN), wide area network (WAN), wireless network, and network-based applications of the company. However, it ensures that information technology services can be backed up and put on online backup for effective recovery of the data. In regardless of whether the business is small or big, there is always a chance for a disaster to come into a business. These disasters can be natural or manmade and to secure the situation, the company requires to set up a vet on network disaster recovery plan as an element. Various natural disasters such as fire, floods, and earthquakes are the major reason for network disasters beyond the scope of the atmosphere for technology failure (Wiatr et al., 2019). Technology failures arise as a result of malicious malware attacks or network administrator incompetence, and any organization should have a strategy in place to recover from such a scenario (Becker et al., 2015). Additionally, many organizations have adopted technology and standards to keep IT infrastructure sound and business continuity.

Ideally, business requires different resources such as staff, technology, and infrastructure. Most of the organizations puts more concentration on the technological front and expect the technology to be the fundamental core aspect of success. Though the technology is considered to be important component of any business, there are some instances and issues that can break the business in a short while (Jorrigala, 2017). Therefore, organization must be ready to guard against any form of disturbance emanating from the technology that could amount to stoppage of business service as a result of unexpected results.

**Setting up Disaster Recovery Plan**

 The most common blunder made by many businesses in modern times is the lack of a network disaster recovery plan, which appears to be both expensive and time-consuming. Companies executives who are on top-line backslide on protecting the company from disasters. Having a business continuity plan carries out the impact of the analysis that differentiates critical and non-critical functions of the network. As a result, any form of impact that may occur before, during, or during the disaster must be included in the plan. In every recovery plan, the budget has to be included to approximate the cost and benefits of the business. Recovery point objective assists in estimating how much data has not been recovered for the company to take stock on data improved and how much has been lost. When a disaster occurs, the company needs a certain amount of time to recover from the loss and carefully backup and plan the loss under some scenario.

**Problem statement**

 When leaders face a crisis, companies without an IT disaster recovery (DR) plan suffer substantial losses, causing significant harm to a business enterprise during a fake or natural disaster. The general business issue is that some managers do not place a high priority on developing IT disruption recovery plans, potentially resulting in millions of dollars in losses. The majority of businesses have failed due to a lack of planning, improper planning, poor testing, inappropriate implementation of technology to the company, and ineffective knowledge management within the organization. These problems have been a threat to many companies based on the network. When a client has the right technology, such as storage craft shadow protect, the organization also struggles to define how to use it. Additionally, a key piece of designing the right disaster recovery plan is understanding how it will be executed and who to be authorized for recovery. The specific business problem is that some IT managers in the manufacturing industry lack effective strategies to develop IT disaster recovery plans to support business operations.

**Literature review**

Many organizations lack adequate DR to safeguard critical data and application software’s. Appropriate DRP reduces risks and chances of disasters of the company. Accessing the work of Iloglu and Albert (2020), the integration of IT with business operations and management are vulnerable to threats that range from computer viruses to natural disasters and deliberate that cat as sabotage. Business continuity plan and disaster recovery plan have played a paramount role to ensure long-term running of the business. Attacks on compromising structures using networks as the key vulnerable weapon have been underway since the internet became a critical component of running a company (Wiatr et al., 2019). Although cyberattacks are the first thing that comes to mind when thinking about information protection, there are certain attacks that aren't done on purpose yet result in significant losses for the company (Edward, 1994). In any case, companies have prepared themselves for the disaster. When unexpected incidents occur, BCP and DRP are the data protection solutions for companies. BCP and DRP are often confused as one and the same, but there is a significant distinction between the two. This chapter provides an overview of contingency plans, specifically BC and DR plans, as well as the distinctions between them.

**Contingency Disaster Recovery Plans**

Contingency plan prepares an organization in terms of responding well on emergencies and its potential humanitarian impact through management tools to all sectors to ensure proper time and effective provision when a disaster occurs. Developing a contingency plan involves making decision in advance about the management of human and financial resources, coordination, and communication procedures. Contingency disaster plan focusses on key process, people, resources, and activities that generates continuity of the operation. The plan has to be always protected from critical and potential vulnerability and threats. When preparing such business practices, operations continuity, and disaster recovery plan events it involves implementation of policies and processes at the organization level. Business continuity consists of plan on actions that ensures regular business will continue even during the disaster while in disaster recovery plan involves restoring vital support system for communication, and IT assets. Additionally, it aims to protect resources and minimize customer’s inconveniences to identify key staff to assign specific responsibilities in the context of the recovery. Contingency plan addresses the following IT security requirement.

1. It identifies functional areas to business operations.
2. Determines how much each situation of a fire or floods would affect the key area and what actions can be taken and the resources needed.
3. Sets goal for return to essential operations.
4. Identifies each required process and document for each step of the process.
5. It implements education and communication plans to keep employees informed to changes.

**Scope**

The scope of this plan is limited to the company network infrastructure to ensure that it facilitate for an alternative in case of disruptions. Such disruptions may be as a result of network or data centers failures, among other technical problems

**Network Disaster Recovery Plans Objectives**

* Serves as guide for an organization IT systems, data centers, internet and network recovery teams
* Provide reference and points network data operation outside this document.
* Provides the required procedures and all the resources needed in the network recovery plans.
* Identifies users and vendors who must be informed in case of the network outage.
* Provide assistance in prevention of confusion experienced as a result of network disruption by documenting, testing, and reviewing recovery procedures put in place.
* Provides for an alternative source of network equipment, services, and power supplies among other necessary sources that would be used in case of network disruption.
* Documenting storage from the data centers and backup plans established as well as for the retrieval of vital network records and other relevant data owned by the organization.

**Nature of the Problem**

Although a good network disaster recovery plan would be beneficial to the business, it is so unfortunate that most business do not have it. Based on the company under consideration in this case which comprises of 100,000 users, among other important information for these users, failure to have ideal network discovery plans would really cost this organization tremendously. The company must consider to have a disaster recovery plan or shutdown in the event of data loss. The company having 2 datacenters and 284 branches mean that this company processes a lot of data on daily basis, which requires to be protected in the event of any unexpected occurrence. With increased competition, a company cannot leave itself behind without having a good network disaster recovery plan. When developing such disaster recovery plan, the company needs to perform cost benefit analysis, to ensure that the budget is within the ability of an organization to implement it.

Undoubtedly, the significance of the problem stated can assessed and measured by its consequence and that of sudden disruption of the services provided by the business. When such services becomes unavailable to the users, they become skeptical and may opt out of such services. After such unexpected occurrence, even if the business will survive, it must pay huge cost for not being prepared for network disaster recovery plan (Jorrigala, 2017). Ideally, there are various aspects of businesses that must be looked at when preparing network disaster recovery plans. Such aspects are based on the data itself, then the other part revolves around having network redundancy if possible. However, it ensures that information technology services can be backed up and put on online backup for effective recovery of the data. In regardless of whether the business is small or big, there is always a chance for a disaster to come into a business. These disasters can be natural or manmade and to secure the situation, the company requires to set up a vet on network disaster recovery plan as an element. Various natural disasters such as fire, floods, and earthquakes are the major reason for network disasters beyond the scope of the atmosphere for technology failure (Rak et al., 2021). Technology failures arise as a result of malicious malware attacks or network administrator incompetence, and any organization should have a strategy in place to recover from such a scenario

**Backup type and policy**

Data backup is a key part both in IT and network plan, and information on a company backup policy and methods. Options of data backup range from dual data centers in different locations that can handle all organization data processing. Data centers run in parallel and synchronize the data between them. Operations can be moved from one data center to another in an emergency. Backup network components are cabling, connectors, power supplies, and spare parts that secures area of company site. Ideally, backup software’s run data copying process while enforcing backup policies of the company. Cloud backup and cloud-based disaster recovery are in-house services. Cloud storage provides low cost and scale capacity for accessibility required. Additionally, while sending information through cloud services, companies are advice to encrypt data to avoid malicious threats.

**Cost Benefit Analysis for Different Contingency Plans**

Disaster recovery planning is very critical for the business continuity and is associated with several benefits for the businesses. Ideally, it include cost saving, which is long-term in nature. With the implementation of effective disaster recovery plans and strategies based on the scenario provided, an organization can recover faster thus avoiding the costs relating to lost revenue as well as lost customers associated with downtime. Additionally, with increased number of users, customers, vendors, partners, investors who interact with the business an effective disaster recovery plan can help in protecting good relationship amidst disaster. The benefits of disaster recovery can be traced through the following:

* Employee Responsibilities and task allocation.
* Organization asset management.
* Testing
* Network management
* Cost savings

**Cost-Benefit on Network Devices**

Based on the budget provided, all the devices provided are meant to ensure there is redundancy in terms of power supply by connecting backbone equipment’s to UPS. Additionally, with the additional network infrastructure provided, they are meant to create redundant network infrastructure such that in case of downtime, there can an alternative option available to ensure services have not gone down. The cost of the network devices required in the disaster recovery plans, their reliability, and cost to replace can be presented as shown in the table below.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Node cost | Reliability  | Time to replace | Installation cost |
| Juniper MX | 200000 | .9995 | 8 hours | 2000 |
| Juniper J | 50000 | .999 | 5 hours | 1400 |
| Cisco NX9000 | 350000 | .9999 | 7 hours | 2000 |
| Cisco NX400 | 250000 | .9999 | 4 hours | 1200 |
| HP 5400 | 40000 | .999 | 4 hours | 1200 |
| HP 3800 | 5000 | .995 | 3 hours | 800 |
| FW Juniper SRX | 20000 | .999 | 5 hours | 2000 |
| IPS | 70000 | .995 | 4 hours | 1500 |
| Local cabling | 100 | .99 | 1 hour | 100 |
| **Total Cost** | **985,000** |  |  | **12,200** |

 Notably, the total cost for network devices as described above will be 985,000+12,200=997,200. However, there are several benefits accrued as a result of implementation of these disaster recovery plan, which is shown clearly on the table (high reliability and time to replace). In the long-run, the benefits will be higher than the cost of implementation, hence it is worthwhile to proceed with this contingency plan.

**Voice Services.**

 Based on this plan, Voice over IP is applicable, and core voice equipment are located in two different cities with full redundancy. The importance of this redundancy is to prevent any form of disruption of the network and systems operations in the event of technical failure, disaster, or downtime by ensuring there is continuity of the service. With redundancy of voice services, the probability of failure is 0.01%.the table below represents the voice services as calculated.

|  |  |  |
| --- | --- | --- |
| Loose due  | 4 hours day | 4 After WH |
| Class A | 6000 | 0 |
| Class B | 2000 | 0 |
| Class C | 500 | 0 |
| Head quarter tower  | 100,0000 | 10,000 |
| Makah tower | 100,0000 | 10000 |
| Madina  | 60,000 | 0 |
| Danmam | 60,000 | 0 |
| Jeddah | 60,000 | 0 |
| Data center | 50,000 | 20,000 |

**Transmission**

 Basically, the transmission network is designed to have a complete redundancy without any single point of failure. If any node fails, it may impact the switches directly those that are connected through it or other users of the building where it is based on.

**Risk management**

 Understandably, risk management identifies, assessment controls threats towards an organization capital and earnings. These threats can stem from a wide variety of sources, including financial uncertainty, legal liabilities, strategic management errors, and natural disaster. Every business faces risks unexpected which can be harmful to costly to the company. Basically, risk management makes the organization to prepare unexpected budget to minimize risks and extra costs before the risks happens. The cost of controlling the risks makes the company to experience loses due to network outage as calculated in the table below.

|  |  |  |
| --- | --- | --- |
| Loose due  | 4 hours day | 4 After WH |
| Class A | 60000 | 5000 |
| Class B | 20000 | 5000 |
| Class C | 7000 | 5000 |
| Head quarter tower  | 1000,000 | 100,000 |
| Makah tower | 1000,0000 | 50,000 |
| Madina  | 700,000 | 20,000 |
| Danmam | 300,000 | 0 |
| Jeddah | 100,000 | 10,000 |
| Data center | 5,000,000 | 1,620,000 |

 The total cost of risk management data center as described will be 5,000,000+1,620,000= 6,620,000. Additionally, other important benefits that risk management play in a company are; creating safe and secure work atmosphere for all staffs and customers, increasing stability of business operations, protects all people involved and assets from potential harm, and establishes organization insurance needs to save unnecessary premiums.

**Incident Response Plan for Branches and Data Centers**

Basically, incident response plan contains set of instructions that assists IT staff to detect, respond to, and recover data from network security incident. Based on the case scenario provided, incident response plan for branches will be different from those of data center. Each data center will be connected to the two backbone routers that can be accessed remotely via SSH in case of any disastrous event. The issues of cybercrime, data loss, and service outage that threatens company on daily bases will be solved through implementation of robust and resilient incident response plan. The company is required to have a plan in case the network failure to prepare customers, vendors, and employees since the network can never be 100% stable and secure. Additionally, when incident response is made available along the disaster recovery plan, it plays a critical role in mitigating any form of damages that may occur during business operations. The designation of a computer security coordinator within the company, as well as other branches based in various locations, can be easily detected through the network. Since business network are complex, the company replicates and stores data in remote location to protect data and network from damage. Accessing the work of Lord (2017), the completion of IT services outage may also be caused by security-related incidents, but service outage procedures can be detailed in business continuity.

**Data Center Environment**

Organization in question has operations in 284 branches and 2 data centers. Ideally, the data center are concentrated in 2 main sites where most activities of the business that are critical in nature are hosted. However, the local requirements and applications needs the platform that is universal in nature to cover the universal requirements as well. The two data centers own by the organization are currently utilizing VMWare’s platform. The application of system hardware has been calculated with the aim of meeting the local business requirements. Additionally, all the sites owned by the company are currently using harmonized hardware vendor, which in this scenario is IBM. Based on the local structure of the organization history as well as the infrastructure, the application of network and storage configurations is an ideal solution to ensure availability and data backup mechanism. Additionally, this makes the hardware platform to be heterogeneous hence making it difficult to maintain. With the application of standardized platform vendor and hardware platform the data centers designed aims to provide an ideal backup mechanism, which is in line with disaster recovery plan for the organization.

**Data Centers and Branches Business Requirements**

The organization under consideration as mentioned earlier has 284 branches. The network configurations need to be stable enough to ensure that the data can be stored easily and accessed whenever needed. Data center operations should be able to provide all the required operations in all branches as well as all the transferable business units. This clearly puts higher and demanding requirements when establishing and designing ideal data centers that that can meet all the business requirements. Such business requirements may vary depending on the business applications, but generally critical applications require the data centers to be running 24 hours in a day, 7 days a week, and 365 days in a year. Summary of most widely used applications within the organization data centers mapped together with organization networking systems can be described as shown in the table below. The key point that can be depicted in this table include the core services which requires the data centers to run continuously to ensure availability even in the case of disastrous event.

Ideally, business requires different resources such as staff, technology, and infrastructure. Most of the organizations puts more concentration on the technological front and expect the technology to be the fundamental core aspect of success. Though the technology is considered to be important component of any business, there are some instances and issues that can break the business in a short while (Jorrigala, 2017). Therefore, organization must be ready to guard against any form of disturbance emanating from the technology that could amount to stoppage of business service as a result of unexpected results.



**Incidence Response Plan Overview**

An incidence response plan comprises of set of instructions that aims at helping IT staff and technical team in an organization to detect, respond and recover from network security or other disastrous events. It outlines steps the company to take upon discovery of authorized access to personal and organization information (Wiatr et al., 2021). The plan codifies the procedures to handle information security related to the incident from detection through the redemption. Ideally, it gives guidance to react on security incident and communication. On bases of roles and responsibilities, it defines various staffs to identify, isolate, and repair data security of the network within the organization. Implementation of business practices reduces the risk of an authorized access through training employees and following appropriate physical security and atmosphere control for technical infrastructure. Additionally, availability and protection of information resources that are managed by the system plays a paramount role in network discovery. The purpose of an incident response plan is to provide successful incident response and to summarize the procedures for dealing with computer security incidents, as well as the tools and communication and escalation routes needed to keep the plan operational.

***Incident manager***

 In network disaster recovery plan, the manager plays part of overseeing all aspects of cyber security incident to ensure proper implementation of the procedures. Employees, vendors, and consumers work with incident managers when they get trapped and need assistance. Incident managers must have technical expertise, access to resources and knowledge, and a customer-service mentality when dealing with users in order to meet their needs. Incident manager also manages lifecycle of unplanned interruptions, malfunction, and quality of reduction of IT services. Notably, the manager records all the issues and designing way to prevent same problems to occur again within the organization. Customers and employees in this case are allowed to utilize technical products of the company. Additionally, an incident manager responds to accidents as soon as they happen, taking whatever measures are required to restore service and return the company to normal operations as soon as possible.

Disaster recovery planning is very critical for the business continuity and is associated with several benefits for the businesses. Ideally, it include cost saving, which is long-term in nature. With the implementation of effective disaster recovery plans and strategies based on the scenario provided, an organization can recover faster thus avoiding the costs relating to lost revenue as well as lost customers associated with downtime. Additionally, with increased number of users, customers, vendors, partners, investors who interact with the business an effective disaster recovery plan can help in protecting good relationship amidst disaster

***Incident commander in field***

Incident commanders are responsible for setting up communication channels and inviting appropriate people into the channel during the incident and training member teams on best practice in case of incident occurrence and communication within the organization. With an incident commander, the communication and teamwork is broken down easily to do duplicate work without any idea in large and complex organizations technology. In the event of disaster, the incident commander manages response activities through assigning personnel and obtaining additional resources required. In this case, when an incident causes damages to an event of company facilities, the incident commander servers as a primary point of contact to support team members to recovery disaster plans and operations.

***Escalation Based on Incident Level***

The escalation procedure based on the incident level comprises of steps to be taken for physical as well as computer security incidences which occur within the 2 data centers and 284 branches. Ideally, the physical security incidences covered in this escalation procedure are meant to provide security and protection of the data centers as well as local sites. Additionally, the computer and network security incidents covered in this section are meant to prevent any unauthorized access of data or any sabotage that could be done to cause system disaster. In this case, the types of incidences can be classified into three levels, which again depends on their severity.

1. The level one incidents are considered to be less severe and only require local systems security analyst be contacted
2. The level two incidents are considered to be more serious and should be handled with a lot of care. Such events should be handled the same day such events occur-this is mostly within 2 to 4 hours of the event. Level 2 incidences must be escalated in any of the 2 data centers to ensure that they are properly handled.
3. The level three incidents are the most serious and should be handled as soon as possible to ensure they have not caused serious harm including system security issues, issues in accessing resources by the customers, employees, among others.

Regarding physical incidents, this may include illegal building access, which is in level 2 incident, property destruction or property theft-which can fall in either level 2 or level 3, among others.

***Classification of Possible Outages into Level Based on Impact and Risk Matrix***

Notably, there several outages that are likely to affect any form of system. Some of the common outages that may occur in any of the branch or in the data centers include network failure, system failure of data transmission, server going down, suspected computer going down, unfriendly employee termination, and loss of personal and organizational password termination sheet, among others.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Likelihood** | **Insignificant**  | **Minor**  | **Moderate** | **Major** | **Critical**  |
| **Rare** | Low acceptance of risk routine management | Low acceptance of risk routine management | Low acceptance of risk routine management | Medium Specific Responsibilities and treatment | High quarterly Senior Management Review |
| **Unlikely** | Low acceptance of risk routine management | Low acceptance of risk routine management | Medium Specific Responsibilities and treatment | Medium Specific Responsibilities and treatment | High quarterly Senior Management Review |
| **Possible** | Low acceptance of risk routine management | Medium Specific Responsibilities and treatment | Medium Specific Responsibilities and treatment | High Quarterly Senior Management Review | High Quarterly Senior Management Review |
| **Likely** | Medium Specific Responsibilities and treatment | Medium Specific Responsibilities and treatment | High Quarterly Senior Management Review | High Quarterly Senior Management Review | High Quarterly Senior Management Review |
| **Almost Likely** | Medium Specific Responsibilities and treatment | Medium Specific Responsibilities and treatment | High Quarterly Senior Management Review | Extremely Senior Management Review | Extremely Senior Management Review |

***Logistic Coordinator***

In any incident response, the work of logistic coordinator it to ensure proper measures are available and organize when there is an incident to work on. In this case of the scenario provided, logistic coordinator must ensure that all tools and any needed support is readily available. Additionally, logistics coordinator must undertake adequate investigations to ensure that all systems for the branches and the 2 data centers and support all the systems security operations. Lastly, logistic coordinator will be tasked with implementing and improving in response as well as resolution of security incidents through automation ore response procedures

References

Becker, M., Goldszal, A., Detal, J., Gronlund-Jacob, J., & Epstein, R. (2015). Managing a Multisite Academic–Private Radiology Practice Reading Environment: Impact of IT Downtimes on Enterprise Efficiency. *Journal of the American College of Radiology*, *12*(6), 630-637.

Iloglu, S., & Albert, L. A. (2020). A maximal multiple coverage and network restoration problem for disaster recovery. *Operations Research Perspectives*, *7*, 100132.

Jorrigala, V. (2017). Business Continuity and Disaster Recovery Plan for Information Security.

Lord, N. (2017). Cyber Security Incident Response Planning: Expert Tips. *Steps, Testing & More*.

Rak, J., Girão-Silva, R., Gomes, T., Ellinas, G., Kantarci, B., & Tornatore, M. (2021). Disaster Resilience of Optical Networks: State of the Art, Challenges, and Opportunities. *Optical Switching and Networking*, 100619.

Wiatr, P., Chen, J., Monti, P., Wosinska, L., & Yuan, D. (2019). Routing and wavelength assignment vs. EDFA reliability performance in optical backbone networks: An operational cost perspective. *Optical Switching and Networking*, *31*, 211-217.

Zamanifar, M., & Hartmann, T. (2021). Decision attributes for disaster recovery planning of transportation networks; A case study. *Transportation Research Part D: Transport and Environment*, *93*, 102771.

Zhang, G., Zhang, F., Zhang, X., Wu, Q., & Meng, K. (2020). A multi-disaster-scenario distributionally robust planning model for enhancing the resilience of distribution systems. *International Journal of Electrical Power & Energy Systems*, *122*, 106161.