THE IMPORTANCE OF DISASTER RECOVERY PLANNING

ANITHA .S

BANGALORE UNIVERSITY

Abstract

The present study focuses on the disaster recovery planning. It provides the causes of disaster recovery plans and its associated recovery processes. This can be of great importance, as there are large number of disaster happening naturally, man-made, preparing for such recovery process becomes crucial in current scenario. Hence the present study focuses on the current aspects of recovery plan.

Keywords: *Disaster recovery, Planning, Process,*

I. INTRODUCTION:

Disaster recovery planning is a technique or a plan that most IT firms having small or large business follows during a calamity. Disaster basically refers to any catastrophe that could result in affecting the business in an adverse manner. Not only every firm should have a disaster plan for it's employees but also to minimize it's loss. In order to minimize a company's loss a recovery plan is important. Now the main question is can we have the same disaster recovery plan for every IT firm or do we need a different recovery plan for every IT or business firm? Every firm has a different asset and a different disaster which they prioritize over the other. It entirely depends on the firm, and what asset is most important to them and how they want to focus on their company's assets. Now one way to do that is by listing down all the things that could result in the failure of a particular organization. This method is called Failure Mode Effect Analysis. What is a failure mode: Anything that takes a company or a business down or any way in which system or a business could fail. Every company has a different failure mode and identification of that mode is very important. While studying business management or any IT related business, Disaster management recovery is a very important subject that should be given more weight. Now the possible disasters any company could have includes natural disasters like earthquake, floods, hurricane etcetera or manmade disasters like fire, theft or server failure. Data loss is also a disaster a firm should pay proper attention to. If taken proper measures the loss can be taken down to the minimum. Let's further talk more about how to handle such risks [1-5].

II. DATA LOSS

Data loss: to ensure a firm does not suffer a lot from data loss make sure there is a complete data backup. For data back up a firm should hire people for data back up plans. Also there are different data loss prevention tools available that ensures that no data from the firm should be mishandled or misused. Also by data loss prevention tools no data of the firm could be accessed by any unauthorized user or a person who is not a part of that firm. Now some firms have a very large business and in order to keep a check on their employees the employers usually follow a very trusted system of compliance which helps in identification of weaker sections of the company. Compliance works as identification of a practice that a firm considers as a breach of company code and takes proper action against the breach. It prevents monitoring and detection of sensitive data for the firm. An example of compliance is some MNC's provide their employees with their own company laptops or PC's and any information regarding to that company cannot be sent to their own email id or out of that system, if done so company considers it as the breach of compliance and a proper action is taken against that person. Also to guarantee the security of one's data remote cloud systems is beneficial. A remote cloud system usually provides all the data back up required for any system. Not only data fed to the computers are relevant but intellectual assets are also very important to be saved. Some companies have BYOD or bring your own device policy. In that case there should be a very secure workforce and

very secure environment in one's company. By using remote data storage sources any firm guarantees a reliable and redundant system for their business. To ensure that there is no leakage of data watermarks should be a major part of every firm's data. It can be taken care of if one tries to perform any malicious activity. Data backup is also required because sometimes we have accidental loss of data. No one in particular can be held accountable for such losses. This may happen due to carelessness or human error or data corruption. This is where data back up is essential or else the whole firm's data could be at risk. If all the above factors are kept into consideration data loss can be prevented [6-8].

III. SERVER FAILURE:

It is another disaster which can be controlled if measures are taken pre hand. For this proper server maintenance is important for stability of the system and the firm to work properly. In order to protect one's firm from a server failure disaster installing an alternate server is also a good option. There are so many factors that can cause a server to fail like environment, airflow between servers, outdated operating systems, Drained systems etc. The server failure can be caused by environment factors like heat. If the environment is too hot and there is no proper cooling between the servers, they can fail. In order to prevent this proper temperature is required and it should be maintained, and servers should be prevented from overheat. If there is airflow between servers, they can also cause overheat between the servers and hence leading to a server failure. To prevent this overflow between servers again a proper and cool environment is required. If any hardware or software component fails it can also lead to server failure. In order to protect a firm's servers from that issue proper maintenance of the system including hardware as well as software components are required [6-7].

IV. OUTDATED OPERATING SYSTEMS:

Outdated operating systems is also a reason that causes a server to fail. In order to avoid this proper maintenance and operating systems updates are required from time to time. Along with all these factors space is an important aspect that should be taken care of. If a system gets out of space server logs can commence all the space leading to failure of server. Improperly installed software is also a reason that causes any server to fail. This server failure not only costs company downtime but also affects the productivity of its employees that means it is a total waste of one's time and effort. If a server is down due to environmental or airflow factors, can take a week or two to overcome these factors. Till then it will be a total waste of company's asset and no productivity leading to a loss for the firm. So the preventive measures that should be taken are proper time to time maintenance, updating the software and an alternative servers for the firm.

V. FIRE:

Fire is also a major disaster that so many firms deal with due to lack of proper systems. The cause of fire could be due to chemical overuse or overheat or due to wood shingles etc. In order to protect the firm from fire hazards we can take preventive measures the buildings can be designed in such a manner that there is a enough space to move out for the employees as they are the main asset of a company. Products like calcium silicate, gypsum boards should be promoted to slow down the fire. Also bricks and concrete should be the major ingredient while making any building. Use of fire sensitive materials such as fire alarms or heat sensors or carbon monoxide detectors. By installing such devices people could be alarmed in advance about any fire conditions. Heat sensors can sense high temperatures and in which the metal changes to molten state that triggers the alarm and let the employees know of the upcoming danger. When there is combustion in air the carbon monoxide detectors detect the gas and triggers the alarms. Also, there should be a practice session for employees so that they do not panic while actual disaster takes place. If in case fire gets out of hand, there should be fire extinguishers in the building along with the fire suppression systems. Also, an emergency exit maps should be installed everywhere in the building. For every firm there should be a fire in disaster plan for the recovery. Every firm should have volunteers for a disaster like this who should know how to use the equipment's involved and how to let people out for evacuation of the building. Mostly in such situations people panic and that causes a even bigger disaster. If all the above measures are taken properly not only disaster can be managed but there won't be much loss to the company [7-11].

VI. EARTHQUAKE:

Earthquake is another disaster in the list which could be managed if preventive measures are taken. The infrastructure of the company if is dome shaped then due to low center of gravity the possibility of the building collapsing would be very low. Shear walls can be made which will resist the lateral forces exerted by the tectonic plates in a earthquake resulting in less damage or no damage in case of a low scale earthquake. Such buildings are formed by association of FEMA and NEHRP along with engineers to form such buildings with a lesser chance to collapse during such a disaster hence less damage. In case of a hurricane we can wrap the buildings with cement or concrete vertically this will protect the walls from effect of hurricane and damages can be minimized. We can also have rust proof metal roof promoting zinc as it is more durable and less likely to corrode. In case the hurricane strikes important resources should be moved off the floor and taken to some place safe. For hurricane prone regions a proper plan like disaster recovery should be implemented and again practice sessions are a must in situations like these. In this case as well some volunteers should be appointed as emergency managers who would take care of all the situations and make sure that no one is in the low lying or a flood prone area. If any emergency occurs, they should be calm enough of know exactly where to go and when to evacuate. Also, people should be calmed so that they do not panic.

VII. THEFT:

Theft is another disaster so many companies have to deal with. Theft can be prevented if proper measures are taken. Like a proper security system should be implemented. Ensuring all the required information is safe. Taking mandatory classes about the compliance for stealing companies' assets. After business hours locking the gates, cabins and doors properly. Develop physical securities and alarms like burglar alarms. Burglar alarms are made by a series of electrical parts which are then connected to a property. In case if any unauthorized access is found they start ringing the alarm loudly and hence theft can be prevented. A burglar alarm beeps for around 20 minutes. It is as loud as a siren. If these measures are taken the risk of theft can be minimized.

VIII. RISK FACTORS

The risk in any organization has to be understood to make the economic frontline to work in normalcy. There are different factors associated with the risk which should be accounted and handled with extra care. The studies have states that risk factors works with business continuity plans along with disaster recovery planning. This influences the management structure and planning strategies [12,13].

CONCLUSION:

This article has so far discussed about all the measures one can take during any disaster. Further if even after the preventions some disaster occurs then the whole team including the employees and the employers must make sure the least of damage by unity and cooperation. Staying united and cooperation is the main source by which one can decrease the risk of disaster. No matter where the company is everyone should know that humanity comes first. No life should be put in danger and employees are the most important part of an organization and should be treated that way. Also, with proper prevention there is no disaster that can't be controlled. A firm let It be large or small, let it be running for a decade or a year needs a disaster recovery plan as well as a disaster management plan. Recovery from a disaster needs a proper plan and then a proper implementation of that plan. Disaster recovery plan includes all the plans for infrastructure, data loss and a proper analysis of everything. If a company had already dealt with a disaster then the company needs a new recovery plan that should not include the past errors and should be effective so that if the disaster occurs any other time the firm should suffer less damage from the disaster.

VIII. REFRENCES:

1. J. Vuong, Disaster recovery planning. *InfoSec '15*. (2015).
2. N. Kanzi, An investigation of the role of records management with specific reference to Amathole District Municipality. (2016).

3. A.Ganji and S. Miles, Toward Human-Centered Simulation Modeling for Critical Infrastructure Disaster Recovery Planning. *2018 IEEE Global Humanitarian Technology Conference (GHTC)*, 1-8. (2018).
4. D.Chandrasekhar, Y. Zhang and Y. Xiao, Nontraditional Participation in Disaster Recovery Planning: Cases From China, India, and the United States. *Journal of The American Planning Association, 80*, 373-384. (2014).
5. Soni, Vishal Dineshkumar, Disaster Recovery Planning: Untapped Success Factor in an Organization (June 16, 2020). Available at SSRN: https://ssrn.com/abstract=3628630 or http://dx.doi.org/10.2139/ssrn.3628630
6. L.L.Hoong and G. Marthandan, Critical Dimensions of Disaster Recovery Planning. *International Journal of Biometrics, 9*, 145. (2014).
7. N.Rogers, K.Williams, M.Jacka, S.C.Wallace and J.R. Leeves, Geotechnical Aspects of Disaster Recovery Planning in Residential Christchurch and Surrounding Districts Affected by Liquefaction. *Earthquake Spectra, 30*, 493 - 512. (2014).
8. N.Okada and E. Yamasaki, Current legislative education within disaster management education. *Japan Geoscience Union*. (2016).
9. Disaster Recovery Annotated Bibliography — International. (2019).
10. M.A. Memon, Disaster waste recovery and utilization in developing countries - Learning from earthquakes in Nepal. *Japanese Geotechnical Society Special Publication, 2*, 143-147. (2016).
11. Y.Xu, X.Chen and L. Ma, LBS based disaster and emergency management. *2010 18th International Conference on Geoinformatics*, 1-5. (2010).
12. Nadikattu, Rahul Reddy, Risk Management in Private Sector (May 2, 2019). International Journal of Computer Trends and Technology, 2019, Available at SSRN: https://ssrn.com/abstract=3629689 or http://dx.doi.org/10.2139/ssrn.3629689.
13. Mohammad, Sikender Mohsienuddin, Risk Management in Information Technology (June 9, 2020). Available at SSRN: https://ssrn.com/abstract=3625242 or http://dx.doi.org/10.2139/ssrn.3625242