Disaster Recovery Planning

Jimmy Vuong
University of West Florida
Undergraduate
11000 University Pkwy, Pensacola, FL
32514
+1 (850) 474-2000
jv24@students.uwf.edu

ABSTRACT

In this paper, the importance of formulating a proper disaster recovery plan is discussed. The disaster recovery plan is part of the contingency plans that organizations create to prepare for adverse events that could affect the productivity or daily operations of the work place. To create a disaster recovery plan, an organization must have an understanding of the use of the plan, the creation process, and the types of possible adverse events.

General Terms

Management, Reliability

Keywords

Contingency plans, disaster recovery plans, disaster, recovery, DRP, Deepwater Horizon

1. INTRODUCTION

In the month of April 2010, one of the most disastrous events occurred in the Gulf of Mexico; the Deepwater Horizon oil rig had exploded and caused crude oil to leak into the surrounding area. The leak was not stopped for months and allowed millions of barrels of crude oil to affect the environment, the wild life, and the businesses located around the Gulf of Mexico. The disaster escalated in damage as a result of poor contingency planning.

Contingency planning is considered to be an "overall process of preparing for unexpected adverse events [7]." The goal of contingency plans are to restore businesses back to their normal operations after a disaster has occurred. Contingency plans can be broken down into four components: business impact analysis, incident response, disaster recovery, and business continuity [7]. Of the four components, disaster recovery should be considered one of the most important parts of the contingency plans to an organization. For organizations to truly have an effective disaster recovery plan (DRP), they must understand what the plan is about, the process of creating the plan, and the types of disasters the plans are for.

Information Security Curriculum Development Conference 2015
October 2015, Kennesaw, GA, USA.
Copyright 2015 ACM 978-1-4503-4049-6/10/15…$15.00.
http://dx.doi.org/10.1145/2885990.2886006

2. EMERGANCE OF DRP

In the 1950s, it was considered to be the electronic data processing era for many businesses. The business world was introduced to the mainframe computer [2]. The mainframe could be considered as one of the early computers only available to businesses because its functions was to record, classify, and summarize the organization's data to their whim [2]. Primarily, the mainframes were used as a backup source because people understood that information was critical and needed to be safeguarded. This method of thinking is considered to be a historic step to creating DRPs. "These activities were the predecessors of DRP [2]."

2.1 Plan Importance

As a result of the past, many DRPs are more intricate, detailed, and cover much more of the organization. Disaster recovery planning is "the preparation for and recovery from a disaster [7]." A proper DRP that has been enacted will enable the organization to restore operations back to normal after a disaster has struck the organization. The Chief Information Officer is often responsible for preparing the DRP because the information technology aspect of the organization is a critical part of the organization that must not be lost or damaged. If the information technology systems cannot be recovered or stored safely, the organization will likely be crippled since those systems are linked to everyday management of the organization's operations, employee information, and customer information.

Furthermore, the DRPs must also include considerations for the physical property of the organization. Information is an important piece to the core of the organization, but the physical property is the home for the information to reside and be used in. Failure to keep the physical assets secured or backed up will slowly, but surely, ruin the organization. For example, retail businesses in Florida understand the importance of protecting their physical store locations when a hurricane is threatening to hit the state. If a store's physical location is too heavily damaged as a result of poor disaster preparation, the store would have to close, move locations, or be rebuilt entirely. All 3 options would impact the organization negatively due to varying degrees of loss profits; however, the options to either rebuild or move would hurt the reputation of the store as well.

2.2 Reactive Plan

On a different note, DRPs are usually reactive; they are not enabled unless an adverse event proved to be too much for the incident response plan to handle. As a result of the reactive role of disaster recovery, proper preparation and creation of the plans must be considered by the organization. There are two important facts that must always be considered.

2.2.1 Required knowledge

The first fact is the expected knowledge of potential issues, environment orientation and implementation, allocation of resources, and the determinacy of roles [4]. The expected knowledge of potential issues relate to any and all adverse events that may happen to the organization as a whole or just in subsections of the organization. The impact of adverse events are unpredictable so having prior knowledge to certain likely scenarios will help mitigate some damages. For instance, an organization cannot accurately predict the amount of damages a hurricane can do to their place of operations; however, having some knowledge of the characteristics of hurricanes (heavy rain, strong winds) will help the organization because they can move equipment around and install window shutters to mitigate the hurricane's damage. The environment orientation and implementation refers to knowing the environment that the DRP will be implemented in. It is not wise for organizations to create a "one-size fits all" plan. A DRP must be specific to the environment that the place of operations is located in. Furthermore, the environment that organizations must be aware of is not just their physical location, but also, they must account for their online presence. The allocation of resources for disaster recovery will always be a touchy subject for organizations.

To implement a proper plan, the adequate amount of investment must be made. The resources that need to be invested are not just money; it also includes time, people, software, and hardware. Money can buy the people, hardware, and software resources; however, experience at properly utilizing all the resources are a different story. The determinacy of roles would help solve the experience predicament. The organization, specifically the Chief Information Officer, should allocate a team that has the experience to create a good plan. This team is called the disaster recovery team. The team should be made up of "key members" of the organization that range from "management, facilities department staff, and others who need to be involved in creating and agreeing on a companywide disaster recovery strategy [6]." Only qualified people should be a part of the team. They are solely responsible for the management and execution of the DRP [7]. After all the preparation for the plan is in place, the organization must consider one final component before the creation of a DRP.

2.2.2 Required needs

The second fact to consider is the task of creating a plan "according to individual needs of the organization or company, including setting of all key parameters [4]." DRPs must be accepted by the entire organization since the plan will incorporate the help of many employees when it is enabled after a disaster has struck. A plan that has been constructed but not reviewed will lead to costly errors during implementation that could further increase the damages of the disaster. As for the parameters to be set, they are the RTO (recovery time objective) and the RPO (recovery point objective). The RTO "represents the maximum acceptable outage time for a business process" while RPO is "the maximum allowable data loss for a defined time [4]." A note to remember is that both parameters do not have to have the same time frame. They can be different depending on the nature of the organization. For instance, a large retail corporation, would likely have a much lower RTO than RPO because the more time the store is left closed, the more profits they will likely lose.

3. PLAN CREATION PROCESS

To actually create a DRP, the disaster recovery team would likely follow an "eight-step disaster recovery process [7]."

The first step is to simply assign individual roles and responsibilities to members of the disaster recovery team. The second step is to develop the disaster recovery planning policy statement. The policy would enable the plan to have the rightful authority to be implemented after a disaster occurs. After the policy creation, the third step is to review the business impact analysis. "The business impact analysis was prepared to help identify and prioritize critical information and its host systems [7]." Reviewing the business impact analysis allows the disaster recovery team to save time by not having to waste any resources on figuring out what is critical and important to the organization. The team can quickly acquire the needed information and go back to creating the disaster recovery plan. The following step is to identify the preventive controls. The team should figure out all the safe guards that have already been implemented by the organization to reduce redundancy. Furthermore, these controls should be measured to ensure that they can actually reduce the effects caused by business and system disruptions [7]. The next step is the actual creation of disaster recovery strategies. These strategies must be thorough to "ensure that the system can be recovered quickly and effectively following a disruption [7]." Some thoughts for organizations to consider as a part of their disaster recovery strategies would be virtualization, backups, and offsite locations [6].

Virtualization would be the use of the cloud computing software to store information on the Internet. The backup thought is the method of storing information at different locations using different storage methods such as USB drives, external hard drives, or actual paper files. Virtualization can be considered a type of backup method as well. Offsite locations are beneficial in terms of having a place to gather data and act as a control center after a disaster. There are 3 types of offsite locations: hot, warm, and cold. Hot sites have data that has been replicated from the primary site. This allows organizations to recover much faster after a disaster because all of the information is intact [6]. Warm sites have similar operating system and applications as the primary site and are used by the organization to restore their information from a previous backup point [6]. A cold site will have just the basics that are needed to run an infrastructure [6]. Usually, the organization must rebuild their systems and then restore their data at the cold sites. These thoughts are an important measure to help ease the damages and costs of a disaster.

The sixth step of the disaster recovery process is the development of the plan document. It "should contain detailed guidance and procedures for restoring a damaged system [7]." This step is important because, in case members of the disaster recovery team cannot be reached, other people can follow the document and restore the system. The seventh step is to test the plan with the use of employee training and exercises. These tests help by finding the errors or failures that occur and fixing them, ultimately improving the plan. The last step to the disaster recovery process is to maintain the DRP; it should be updated regularly to incorporate new technology, methods, or personnel.

4. DISASTER TYPES

DRP helps businesses recover from adverse events. There are currently 3 types of disasters that could affect normal business operations for an organization. They are called “natural, technical, and human inflicted disasters [2].” Furthermore, these 3 types of disasters can be classified as either rapid-onset or slow-onset disasters.

4.1 Natural Disasters

Natural disasters are events that happen as a result of nature; these events cannot be prevented. Some examples of natural disasters would be floods, hurricanes, tornadoes, snow storms, and earthquakes. Natural disasters have the capabilities to cause massive amounts of destruction to physical assets; however, not all natural disasters will hit a single business location. Some disasters are area specific in the world. Hypothetically, all of the United States can experience rain, but only the northern states can expect to have frequent snow storms because the northern areas are generally much colder during the winter seasons.

4.2 Technical Disasters

Unlike natural disasters, technical disasters are events that occur from hardware or software failure. They generally cause some physical damage to the organization if the hardware needs to be replaced after the event, but software failure resulting in information damage is the most important part of the technical disasters. These events are information technology related and such examples would be system freezes, hardware crashes, and connectivity issues. This type of disaster is most easily preventable with adequate monitoring of hardware capabilities and software updates. The only way for true technical disasters to massively hurt any organization would be if the organization was negligent.

4.3 Human-Made Disasters

The last disaster type, human-inflicted, have great potential to be very devastating to any organization by having the ability to cause both physical damage and information damage. Some reasons why human inflicted disasters would occur in the beginning would have to be by employee negligence or corporate sabotage by another organization. Improperly trained employees can accidently or intentionally destroy physical assets while working or input incorrect information that can lead to costly errors in the future. In corporate sabotage, an organization actively tries to destroy an opposing organization by causing destruction to the opponent’s physical location or by launching cyber-attacks that can lead to information theft or loss.

4.4 Rapid-Onset and Slow-Onset Disasters

Rapid-onset disasters “occur suddenly, with little warning, taking the lives of people and destroying the means of production [7].” Slow-onset disasters “occur over time and gradually degrade the capacity of an organization to withstand their effects [7].”

The recent event of the Deepwater Horizon oil spill is a good example of rapid-onset and slow-onset disasters that inflicted devastating damage to British Petroleum (BP). The Deepwater Horizon oil spill occurred at the “Macondo well in the deep water of the Gulf of Mexico” and was the “largest accidental oil spill in the world [1].” The reason for the spill was a result of crude oil and mud entering the drill head pipe and flowing upward toward the oil rig. Once at the rig, the crude oil ignited and caused an explosion that sank the rig and damaged the well head. The well head was left unplugged for several weeks and allowed an estimated “4.4 millions of barrels of oil” to flow into the surrounding areas [1].

The reason for such a disastrous spill was thanks to BP’s negligence. They did not follow a proper plan creation process. Their response plan (disaster recovery) for the Deepwater Horizon oil rig were just “boilerplate copied from plans designed for use in the Arctic [1].” The plan stated that the company had many resources in place at strategic locations if a spill ever took place; however, when the spill occurred, the company was seen flopping around and hiring any boat and personnel to help clean up the disaster. Even the former CEO of British Petroleum, Tony Hayward, admitted on an interview that the company “was not prepared” and was “making it up day to day” when the spill occurred [3].

To conclude, there was no concrete DRPs, no disaster recovery team, no resources, and, most importantly, no one from the company thought it would happen. DRPs are reactive plans that are created to mitigate the “what-if” events. If BP implemented a good DRP, the rapid-onset disaster (oil rig sinking and crew’s lives lost) would have potentially been mitigated to a great extent and the slow-onset disaster (largest oil spill in history and billions of dollars in payments) would have not crippled the company. BP had to sell off large chunks of their assets to stay in business [5]. The decrease of oil sales did not cushion their fall either.

5. CONCLUSION

Contingency plans are very important to the survival of a business in the event of a disaster, especially the disaster recovery plans. Good plans will save the company because such plans are very detailed. It is better to be prepared and ready for adverse events than left wondering what to do after an event occurs.

6. REFERENCES

[1] Griggs, J. W. 2011. BP Gulf of Mexico oil spill. Energy Law Journal, 32(1), 57-79.

[2] Hoong, L. L., and Marthandan, G. 2014. Critical dimensions of disaster recovery planning. International Journal of Business and Management, 9(12), 145-158.

[3] Mejri, M., and De Wolf, D. 2013. Crisis management: lessons learnt from the BP Deepwater Horizon spill oil. Business Management and Strategy, 4(2), 67-90.

[4] Pinta, J. 2011. Disaster recovery planning as part of business continuity management. AGRIS on-Line Papers in Economics and Informatics, 3(4), 55-61.

[5] Reed, S. 2014. BP’s earnings fall as it continues to sell assets. The New York Times. http://www.nytimes.com/2014/04/30/business/international/bps-earnings-fall-as-it-continues-to-sell-assets.html?_r=0

[6] Samara, L. 2014. Disaster recovery: Executing the plan. PCmag.Com. http://www.pcmag.com/article2/0,2817,2409510,00.asp

[7] Whitman, M. E., and Mattord, H. J. 2014. Management of information security (4th ed.). Stamford, CT: CENGAGE Learning.