Disaster Recovery Plan Creation for GiveChance Foundation

Brian J. Morales González
Computer Science
Juan Ramirez, PhD
Department of Electrical & Computer Engineering and Computer Science
Polytechnic University of Puerto Rico

Abstract — *GiveChance Foundation is a non-profit Foundation created for helping children born with health problems through the help of sponsorship. The Foundation helps serve children from a week born up till the age of 13, having already helped over 15,000 cases of heart diseases at birth. GiveChance Foundation has been working with children since the year 1998, but has yet to make a plan for the case of a disaster. Employees are driven to help each individual case. They offer orientations on medical resources such that if not available in Puerto Rico, they may go to the U.S. to have their treatment free of cost. They did not deem having a safe place for their backup files as an urgent matter, and left them in an unsafe area, stretching out personnel to other areas. Recently, this foundation had suffered from losses due to a flooding of their facilities, having many patient records damaged and unreadable. This project seeks to devise its disaster recovery plan.*

Key Terms — *Backups, BCP, Cloud Computing, DRP*

INTRODUCTION

The GiveChance Foundation had found itself in a delicate situation. The registry office of the GiveChance Foundation was found to be unable to perform its duties and has brought a situation in which many aspects of the job were halted in order to better establish future services and a better investment against future contingencies. These services needed to be restored as soon as possible. This makes evident the need for a plan to help control these situations. Even if many people do not even bother to consider some events that may take place, it is always a good idea to have a plan for such an occasion to prevent a catastrophic loss of data or damage. A disaster recovery plan (DRP) is an important asset to any business, and a logical one and should be included in this setup. A DRP is considered to be a plan that goes step by step in order to get a business running its operations normally once again after a disastrous event has taken place. The following demonstrates a plan to help re-establish the main function of the GiveChance Foundation's main services.

CONTINGENCY PLANNING TEAM

To tackle this disaster, we shall devise a Disaster Response plan and Contingency Planning team to help prepare against future unexpected events, since the Incident Response Plan would not cover a scope this large. The project leader shall coordinate the actions to be taken for the duration of the disaster recovery plan, until operations can continue normally. This colleague shall be named by the authorization of the foundation's board of directors, to follow a strict schedule and assessment of the damage done in the registry area. For the time being, it shall be the responsibility of Brian Morales, a senior network administrator and consultant for the foundation, and the individuals he decides appropriate for this task. The other individuals appointed this responsibility shall follow a plan that outlines the maintenance of operations, recuperation of operations and its continuity within a timetable in the different aspects that may have occurred in the disaster. The general outline of processes to be carried out can be seen in Figure 1.

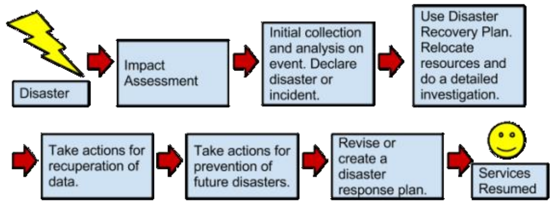
Disaster
Impact Assessment
Initial collection and analysis on event. Declare disaster or incident.
Use Disaster Recovery Plan. Relocate resources and do a detailed investigation.
Take actions for recuperation of data.
Take actions for prevention of future disasters.
Revise or create a disaster response plan.
Services Resumed

Figure 1
Disaster Recovery Process

Aspects include structural damage to data systems, and protection against malicious attacks, hardware failure, software failure, bad upgrades or corrupted data, human error, or nature. Reference [1] demonstrates four typical ways to get running normally once again:

- **Data Backups:** hard drive or tape backups which will probably not contain recent data and are usually contained onsite or offsite. This is the most commonly used for restoring services.
- **Electronic Vaulting:** sending batches of data to an offsite facility through secure connections.
- **Remote Journaling:** only current live transactions are transferred to another location in real time. No stored data is involved.
- **Database Shadowing:** the combination of electronic vaulting and remote journaling, it duplicates live transactions and archived data onto a redundant server offsite.

Backups are not only good for disaster recovery, but also very important for archival or operational purposes. They are also good for accidental deletion of important data. As for the solution for GiveChance Foundation, we will have to rely on database shadowing based on a cold backup, since the backups that were present at the location were damaged. According to reference [2], a cold backup is one where applications are not active while the backup process is in effect. We would have to make a full backup to get back most data lost. All backups should also be checked to have the correct hash number.

Plan Setup

The recuperation of data takes precedence over all other tasks, as this is the most important asset the foundation contains. In the case of having structural damage in the facilities, it is to be evaluated immediately for deciding upon the equipment’s relocation. Sensitive data such as patient social security numbers carry an additional risk of being exposed and should also have their own sets of countermeasures against future attacks. This is a situation that is greatly desired to be avoided, as this can bring about law suits and defacement of the GiveChance Foundation. The project leader shall take the newly created system and analyze it in an outside location.

The established area is up to the project leader but it is desired that it be handled without disclosing it to the public and on official campus ground. If the project leader has decided to break the team into sub teams, they should all have the consent of the project leader when working on their part of the incident. If a future incident is found to occur on a weekend, the team is needed immediately regardless of the situation. Reports must be created in a clear and concise manner, such that anyone can understand what exactly is needed even if they do not understand what has taken place. The board of directors is to approve of all procedures and project plans that will be taking place in the offices of GiveChance Foundation. The approved agenda is to be administered immediately. In the meanwhile, a temporary solution may be implemented if the records office feels the need is too heavy. Assumptions of alternative ways to get the work done may also be taken under consideration by the consent of the director of the records office.

Long term project leaders and teams shall be taken under serious consideration as a full time job within the company. The point in which these are assigned is determined by the board of directors after careful consideration. Training for these employees shall be devised, although previous experience is preferred. All project leaders and those that also integrate as the team must keep all knowledge undisclosed for any reason. Their signature shall always be required once on the team and once leaving, knowingly admitting to non-disclosure of any way or form of information enforceable by the law.

The project leader is to identify the current functions being held at the registry office. The functions may vary from time to time, so different activities may hold different weights at certain points. These activities might be tied to certain information systems, so it might be a good idea to talk to the personnel that support this team. This can help immensely and help shorten guessing work on searching important areas that might have been affected and how it is supposed to look. On the other hand, interviewing for other purposes such as coordinating objectives set or marketing may also be worthwhile. After questioning some of the areas that are of great concern, you can get an idea of what type of processes are more critical than others. This can lead to the creation of an impact analysis. A business impact analysis is [3] "… likely to identify costs linked to failures, such as loss of cash flow, replacement of equipment, salaries paid to catch up with a backlog of work, loss of profits, and so on. A BIA report quantifies the importance of business components and suggests appropriate fund allocation for measures to protect them." Brian Peterson [4] goes on saying "the process for most BIAs should start with the development of an application portfolio. This identifies the applications that support specific business processes like "payroll," "supply chain" or "order to cash." The BIA study then should determine the likely failure points for the components defined in the portfolio. Next, the examiner should determine the cost of such failures. The cost is often measured in expense per hour but, depending on the business process being evaluated, may instead be defined by share price, the impact of a mission failure or even life and limb." Since this is the registry office, it is safe to presume that payroll is not a direct part of this plan since they are separate tasks. Instead we have the process of registering patients and maintaining a record for patients, and so on. All delicate information must have special attention.

As you continue to identify critical equipment, it might be easier to develop a chart which outlines the weight they carry. It is a good practice to do this to know what needs greater attention in the least amount of time. It also proves to be a better way to organize your thought. This chart should scale what is important to what is merely a desire, also containing how much time it is able to be down. Considering the registry office has such different dynamics taking place at different times, it is important to consider the time that it is able to be down. Other areas that might be of use are analyses of the current physical security. This may include from where you enter into the registry office, to where the employees enter, how it is locked up when nobody is working, how there equipment is stored, and who might have access to entering.

As well as employees, others who could be affected must also be considered. This includes contractors, temporary workers, volunteers and the general public. Backups should be taken into great consideration as well as these might be one of the only ways to recover important data or processes. It should be able to execute as expected, and not encounter troubles of having stored the information incorrectly or also being affected like the main systems. It should also be stored in a place where it will not be affected by damage. Data security must ensure data is stored correctly with a way to know that its integrity has not been changed, by using some sort of hash calculating function or encryption. Levels of privilege should also be taken under consideration as this makes for avoiding unnecessary people viewing information that is delicate. For some processes, the use of biometrics could help for prevent future intruders gaining access to information. As mentioned by reference [5], biometrics are "security measures provided by computer devices that measure physical traits that make each individual unique". They use special components that digitize and compare your traits such as voice or finger prints. This high tech procedure is one that is rapidly gaining attention as there is no need for password memorization. However, it might become tedious when this method fails because of a lack of personnel availability or changes within our bodies. Regardless of its use, all connections to the work group in the registry office must be secured. If an employee has decided to leave, it is the responsibility of everyone to change their passwords and secure the building with different measures such as different keys, logins, etc. Disgruntled employees may also be a cause of damage to systems inside the registry office. Even if they were transferred, it does not mean that security is still strong. They might unknowingly convey information or use methods themselves to try and gain unauthorized access. Since employees form such an important part to an office, it is also of importance to maintain strict policies and guidelines for how an employee is to act. Maintaining these policies is a great practice as they come in handy if any legal action were to occur. If natural actions were to occur such as a tornado, hurricane, earthquake, thunder, it should be identified what measures are in place. The locations of the mission critical applications are an important aspect that may be under looked. Take special notice of details such as excessive humidity because it may damage the system because it was not designed to work under those conditions. Some mission critical functions are not even given the proper attention. These are to be identified as without them it would incur in a tremendous cost for GiveChance Foundation. Calculating the probability of system failure or disruption might be hard to explain if it has been working fine for a long period of time, but it is necessary. A rule of thumb to calculate this is through a probability prediction. As reference [6] tells us that this is similar as how an insurance company would calculate a teenager and the likelihood of a car accident, which is rated by the rate his peers are having accidents. The measures that are appropriate should be taken so that there is no chance for having an incident present. Once this information is gathered, it is time to move on to preparing a security analysis.

The appointed individuals to each task are very important. The project leader may decide that the incident calls for different teams to tackle different tasks. If he wishes, he may break his team for tasks specifically detailed for communications, facilities, applications, hardware, or functions that have been also seen as critical. This approach might be a more sound approach considering the weighted chart. If the chart has been detailed that it needs its focus on just one critical service, this plan might not be the appropriate one for the occasion. Depending on what is needed, the allowable delay might not be viable. The day that the crucial operation is needed might be one that requires a heavy processing. This also introduces the need for making a workflow for each task, a step by step process detailing the completion of a process. For a better explanation on how it is to be detailed, each person handling the task at hand should identify the system by its type, component name, frequency of use, run time, and its allowable time that it will not be in use. If working with a storage system, the records that are of importance should be known and described. Inside its description, there should be a name, what kind of document it is, where it is being kept on storage, where it originated from and its backups. Backups descriptions include how often there have been backups, by what means (on campus or in another location), how long was the document retained and who has access to it.

Once evaluated and described, it is safe to assume that the team can make an assessment of what might have gone wrong and what is the procedure that follows. For example, it might have been faulty hardware, so a replacement might be what is needed. Whatever the team finds is the needed requirement, it should be described by name and type, its vendor, and location of where to find it. This will greatly help with organizing the funds needed to do the adequate fixes. It does not always have to involve a cost though. Sometimes what needs to be fixed can be solved by other means that would not involve purchasing a new part or equipment.

In many cases, a manual approach can be used instead of an automated one. In the case of the registry office, it may be documented by hand the processes that they think can be done by it. Later on they might decide on entering the data by updating their automated storage and processing methods. While this might be temporary, it might also be slower and more tedious to implement. If another system can be used, such as a type of mobile application that could also access data, it might be more viable.

There is also a list of people that should be considered that will be contacted. Such individuals may include the supervisor or secondary colleague appointed to be contacted if the system is not operating as it normally should. They should be able to identify what is needed for the system to restore its working order and what processes could be done for the recovery of data. They may have a better vision of the system than most other people. The vendor can also be considered an individual whose support may prove to be invaluable. They should also be able to give out clear instructions on how to access main functionalities to the system as well as its protection. Vendors however, might not be so responsive if the system has undergone incremental changes to meet the needs of GiveChance Foundation. They might also require you to have a receipt of purchase for giving out their services. While it is possible that the primary colleague appointed to maintain the system has this information, it may be a contract that was only for a temporary time. Thus, all support must be addressed with the most amount of information obtained possible for the best effectiveness of support. The team should make an effort of finding manuals online also if they are not in possession of one. Each team should later document how they will approach the task at hand, the time needed for recovery, and the priorities they have found for recovering the functionality expected. This should be outlined in a schedule that portrays the work to be accomplished. It needs to be as realistic as possible. Many use a Gantt chart or equivalent software to portray this. After finished with this, the project leader will re-assign who will deal with what situation.

There might be a team just for the planning aspect of recovery procedures. This team might want to verify for offsite storage facilities and backups or, if adequate, organize for one. The records that they deem need more protection such as processes and system instructions should also be handled with care. But before they get to handle this, they should present it to the project leader for approval. He shall determine what the most viable route to precede taking is, as having an offsite storage facility might be a bigger task than what the recovery scope covers at the moment, for example.

If damage that was done or identified is beyond repair, it could be viable to use an alternate site. This site would handle the needs depending on how crucial they are. Assessing the requirements should be considered before choosing an outside site. If the needs currently lie within a system that is crucial to be operating at all moments, an outside site called a hot site might be a good solution. However, the site may only be compatible with a certain system such as Windows, Macintosh, Linux, etc. They may not have the availability of certain software either. It is of great importance to consider every aspect of an outside site and consider alternatives. In some cases a cold site is a better route for a more long term stay caused by greater damage. It also is a lot cheaper, which brings up another point. A hot site is very costly per day. If on a budget, this alternative might prove to be not as beneficial as others. It might not even contain the environment you wish to replicate for business continuity. Regardless of the preferred site, Figure 2 mentions some characteristics that should be desired from the cold or hot site.

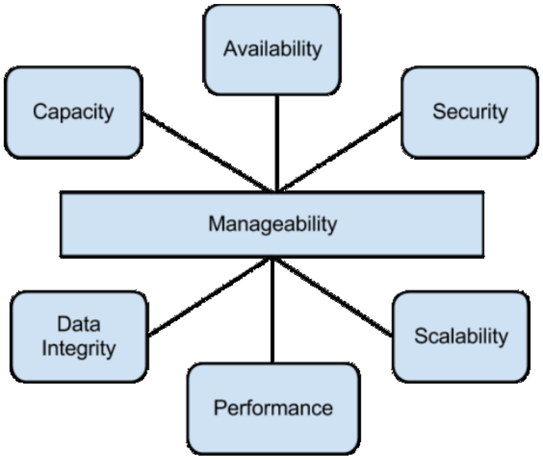

Figure 2
Desirable Traits for Cold or Hot Site

It is hard based solely on benefits to come to an agreement that an outside site is the best solution. Once taken into consideration, it should be presented to the project leader for his approval. He will then present what is the best alternative to the current situation and how it is best addressed. The board of directors takes into consideration what is to be done.

In order for an emergency to be established, it must fit a certain criteria. This criteria is determined by the project leader if he finds the situation will not allow for business continuity. If a resource for the registry office is not available for use by something preventing it from its availability when needed, it is an emergency. If a natural disaster hits GiveChance Foundation, it is a temporary emergency that might damage the resources. Even if it is a plague of sicknesses that is spreading, this also involves an emergency because work cannot be completed under these conditions. Humans can also cause an emergency by creating an error unknowingly on the system. This can be caused by a variety of factors. However, some individuals do it on purpose knowing some vulnerability that might affect the system. This is known as sabotage and it can really deface a company. Other types of human attacks are viruses, Trojan horses, spam, key loggers, worms, and spyware, amongst others. This accounts for many computer systems, but can be prevented as this is a normal type of attack. Intrusion detection systems and intrusion prevention systems should also be up and running for daily operations. Fires and excessive moisture in the air are another thing that can occur, damaging the precious data. Hardware and software can also suddenly not operate correctly also affecting the system. Solar flares that cause electromagnetic interruptions to electronic services could also be a potential cause of worry, but can be remedied with locating sensitive equipment in a special facility. Any one of these may be considered an emergency situation.

During an emergency, all steps taken to respond to the emergency incident should be written down including before and after. Some techniques for assessment can also be prepared and the state of emergency should be declared. The safety of all human beings is and should be the priority before all else. Vendors and university officials should also be notified when possible.

Table 1
GiveChance Foundation Disaster Data Recovery Plan List

Data Personnel:

Name	Address	Position	Telephone

Table 2
GiveChance Foundation Disaster Recovery Plan List

Applications:

Application Name	Manufacturer	Fixed Asset (Y/N)	Critical (Y/N)	Used Daily, Weekly or Monthly

Table 3
GiveChance Foundation Disaster Recovery Plan List

Inventory:

Manufacturer	Model	Serial Num.	Leased? (Y/N)	Cost

The identification of all employees that are present is a must. Once knowing this, it can then be an admirable idea to have the recovery team gather and be placed with certain roles or responsibilities. Now comes the identification of vital records. This should be described in categories. All damaged equipment found should also be documented, as for when talking to the vendor it is easier to talk on the losses. All equipment that is still in working condition should also be documented and verified adequately. Software that was being utilized up to that moment also belongs on the list of things that need to be documented, as these are one of the main tools for executing the procedures necessary. Any additional software that might have been used for using a recovery is also important to document as this might be a very valuable asset to have for recovering. If there was ever in existence a list of the vendors, it is the time to start searching for it as this also helps get down to what other equipment might have been lost. As demonstrated in Table 1, Table 2 and Table 3, arranging an organized list will prove better. There might also be a list of the terms of use or restrictions that the vendor is willing to help or replace with. The communication lines that were also necessary should be documented as well. This also goes by hand with the equipment that was being used as this is what the ports on a system might have used.

Now considering all of these items, it is a wise idea to analyze well what it is that needs to be done to continue operations and what criteria must be met for it to return to normal. This should mean that whatever backups were done of the system should be utilized to recover what has been lost if that is the case. If this means structural damage, than that means how to fix the areas of the registry office so that it can be safe again. If this means using a manual method versus an automated method, what are the things necessary for this to be a viable action? All things considered, maybe it is a good idea for the use of a cold site, hot site or warm site. Contacting vendors that will help you will also prove helpful for the replacement of those systems that have been lost or damaged. If new purchases are needed, than there should be a series of testing and training involved for its correct implementation. It should be tested under the most realistic situations.

After the new equipment has been tested and implemented, it is important to also document everything that has happened. Maintenance is something that can’t be neglected. Reference [5] tells us it is also a good idea to implement audit trails. Audit trails is the presence of documentation that can be followed back to its previous information stages. Another thing to consider is if at any point, there was equipment upgrades, a new inventory list should arise from the newly installed equipment. In the case of a sickness, maybe it would be advisable to also install a new mobile form of the same applications that are necessary, or count on a type of cloud storage that contains privilege levels of security. Cloud computing consists of having resources become available over the internet and may include applications and storage usage. Cloud computing is very useful for having business continuity. A new disaster recovery plan should be devised, and with it new procedures that detail the avoidance of such a disaster or how to tackle it for damage mitigation. All network diagrams should be implemented once again. If any staff was found hurt, a call to their family members is in order. Depending on how grave the injury has been, it calls for the use of the pension plan. If any staff was found dead, this also applies for a call to their family and a pension to the affected family. The pension plan may be claimed with the director of the Human Resources office. GiveChance Foundation is also insured for natural disasters to its campus, so if the damage that has been done was towards the structure of the building, it can be claimed. All other services may be restored after all has been set and done

CONCLUSION

Once undergone everything and everything has taken its place once again, the plan should enforce the use of a maintenance plan that reviews newly designed upgrades in technology that may be applicable to the situation, procedures that might have changes involved and need updating, among other technologies. Maintenance should also include the modification of some procedures if they are not as effective as they once were or if they are no longer needed. Updates to newer versions of software should also be programmed to happen automatically. All of these changes should always be consulted first. Finally, a time should always be taken for creating reviews on the system as a whole. It should not be something that happens at the last minute before an incident has occurred. A good auditing should cover all aspects of importance for a well-executed plan on the good maintenance of the systems. It does not guarantee a complete protection from everything, but as far as mitigation, goes it comes in handy. Controls should be placed where needed, and the revision of these controls should also be accomplished within an adequate period of time or after an event has occurred. Encryption of sensitive data should be implemented. IDS and IPS should be considered measures to help mitigate attacks on a system, but not prevent them entirely. Forensic controls may also be considered if the systems affected involve sensitive information. Redundancy is to be made sufficiently available by tape backup. A contemplated cloud service for redundancy is still in the process of being approved. If the disaster taking place requires it, a manual operation might solve the problem temporarily. The relocation aspect must be contemplated well before doing any type of issuance. For the case of relocation of the registry office, it is advisable to consider a cold site, if not during the time of its heavy processes, as to not incur in incorrect use of resources. A warm or hot site might also prove effective if during the times of heavy processing, but not if it is the opposite. Currently, the registry office could temporarily be located into another location within hospital grounds as they have been linked to each other for some time, such as a few rooms, if the necessity is heavy. The affect that this causes, depending on timing, varies. It might become troublesome, however, as these places are needed by the faculty and patients.

While no disaster plan is a complete foolproof plan, it should help in recovering the operations that take place. This is a guide for contemplating the measures that have to be accomplished and analyzed. With this in mind, it is incredibly important to keep a disaster recovery plan up to date. Without a disaster recovery plan, GiveChance Foundation is under the risk of vanishing entirely from being a business. As long as all the right measures are produced and made available, everything should proceed as normal. This document should be placed in the hands of the board of directors, the director of the registry office, and the disaster recovery project leader. Amounts of equipment change, so a list of all equipment available should be rechecked every 6 months. Backups for all equipment should also be planned at least daily if in times of heavy demand and at least every 3 days if not in heavy demand. Manual procedures should always be contemplated and equipment should have its own backup power source and adequate conditions for operation. Plans for safely dispatching individuals should be considered highly, taking the information assets as a second priority. Hopefully, this will help make GiveChance Foundation a more secure and better implemented business.

REFERENCES

[1] Whitman, M., & Mattord, H. (2010). Planning for Contingincies. Management of Information Security (3 ed., p. 97). US: Cengage Learning 2010

[2] Somasundaram, G., & Shrivastava, A. (2009). Chapter 12 Backup and Recovery. Information Storage and Management: Storing, managing, and protecting digital information (pp. 251-280). Indianapolis, Ind.: Wiley Pub.

[3] Miller, K.(2005, September 1). What is business impact analysis(BIA)? – Definition from WhatIs.Com, Storage Technology information, news and tips – SearchStorage.com.Retrieved April 19, 2013, from http://searchstorage.techtarget.com/definition/business-impact-analysis

[4] Peterson,B. & Contributor(2008, October 1). Business impact analysis. Storage Channel information, news and tips – SearchStorageChannel.com. Retrieved April15, 2013, from http://searchstoragechannel.techtarget.com/feature/Business-impact-analysis

[5] Brien, J. A. (2001). Chapter 11 Security and Ethical Challenges of E-Business. Introduction to information systems (10th ed., pp. 474-480). Burr Ridge, Ill.: Irwin.

[6] Young, C. S. (2010). Metrics and Methods for Security Risk Management. Amsterdam: Syngress/Elsevier.