

Managing Disasters: Forming, Preparing and Testing the Disaster Recovery Plan (July 2006)

Stephanie D. Hight, *CCNA, RHCT*

Abstract— Disaster Management is a wide-ranging subject that encompasses disaster prevention, disaster management and disaster management control. The purpose of Disaster Recovery is to respond to disastrous events and to have a fully operational plan ready to be put into place. Disasters are something that an organization cannot afford to not be prepared for. As firms grow more dependant on uninterrupted information system functioning, disaster recovery is receiving increasing attention, and a growing number of organizations are beginning to engage in Disaster Recovery Planning. Preparing a Disaster Recovery Plan can be a daunting task for an Information Technology Department that has not had to think about recovering vital systems before. The Disaster Recovery Plan itself should be clear and concise and able to be understood at any level of knowledge. A key concern in the management of disaster recovery is that mistakes do not occur in the recovery phase. A realistic disaster exercise is where the disaster recovery team will gain the most mileage and make the most impact in a number of areas. Tests and exercises are vital sources of feedback and short of experiencing a real disaster they are the only way of ensuring that the recovery plan will work.

Index Terms—After Action Report, Cold Site, Disaster, Disaster Recovery Plan, Hot Site, Recovery Time Objectives, Warm Site.

I. INTRODUCTION

THEY are something that we never want to experience or go through, but something that companies and local governments have to be prepared for. Disasters; the word can conjure up a lot of images and bring fear to the most capable of IT Departments. They seem to come in many forms. Natural disasters such as tornadoes and hurricanes are well known for causing a great deal of harm with the most recent example of this being Hurricane Katrina. But there are also a great number of other disasters that can cause the complete upheaval of an organization, it could be a local disaster within the building that the company resides in and be something as simple as an electrical malfunction in which the sprinkler system goes off and all electronic equipment has been rendered useless. Whatever the cause of the disaster an organization needs to be prepared and know where and when

it can get the systems back up and running so that the interruption in business can be as minimal as possible. A Disaster Recovery Plan has become more prominent since September 11th, and even further re-enforced for states and municipalities in the recent destruction of New Orleans through Hurricane Katrina. States and municipalities have a great responsibility to the citizens it serves and the people they employ to have a well laid out plan. Citizens will naturally look to the local and state government for direction in the event of a disaster and IT systems need to be available to support the aftermath. This paper will attempt to define and discuss the importance of having a Disaster Recovery Plan from the Information Technology perspective, as well as the essentials that need to be included in the plan. It will also discuss the inter-dependence and ability to work together in getting the systems back up and running at the original site or some other designated place. This paper will include tips in choosing the team that will be responsible for recovering all essential systems and the criteria that is placed on what systems need to be recovered in what order.

II. THE DISASTER RECOVERY PLAN

Disaster Management is a wide-ranging subject that encompasses disaster prevention, disaster management and disaster management control [1]. Although this paper will only address the management of a disaster from the perspective of Information Technology, it is important to note the much wider perspective that an organization needs to take when beginning the ongoing project of Disaster Recovery. The purpose of Disaster Recovery is to respond to disastrous events [2] and to have a fully operational plan ready to be put into place. These disasters could come from natural causes and in some cases can be predictable seasonal events [3], but in most cases they are not. They could be defined as anything that causes a large disruption in services that Information Technology provides. Disasters are something that an organization cannot afford to not be prepared for. The City of Raleigh in North Carolina has been developing their Disaster Recovery Plan since 2001 and DJ Hess, CISSP and the City's Information Security Administrator sees the role of IT as the lead in the Disaster Recovery Project. Hess states "The role is critical by default and need. Everyone will complain about IT but when the need arises, they are on the doorstep waiting for the restore to happen as quickly as possible. IT is the lead on

Manuscript received July 17, 2006.

Stephanie Hight is a System Administrator with the City of Raleigh, Raleigh, NC 27601 (e-mail: Stephanie.Hight@ci.raleigh.nc.us).

the DR planning, implementation and testing along with the application owners.”

As firms grow more dependant on uninterrupted information system functioning, disaster recovery is receiving increasing attention, and a growing number of organizations are beginning to engage in Disaster Recovery Planning [4]. Preparing a Disaster Recovery Plan can be a daunting task for an Information Technology Department that has not had to think about recovering vital systems before. It is not an easy feat, but one that must be approached with great organization and with the mindset that Disaster Recovery Planning is not a linear task, but rather a cyclical one. It should be regarded as a dynamic process, one that is continually evolving and improving as the organization and environment changes. The plan should be ever changing and reflective of the current environment that exists. It is not something that once complete will sit on a shelf and never be updated or changed.

In the initial phases of the Disaster Recovery Project, it should be decided as to what type of site the organization should have, cold, warm or hot. A cold site is defined as an alternate site that can be used by an organization if a disaster occurs at the home site. It contains rudimentary services and facilities. A warm site frequently includes computing equipment and peripherals with servers but not client workstations. A hot site has systems that are identical or similar to a home site for use after a disaster, this site runs synchronously with the home site with immediate data replication [5]. The site a company chooses will largely depend on the size and budget of the organization and the speed at which it needs to have business running again. A large national organization might not be able to afford losing business if a main office goes down, so they would choose a hot site that could be immediately switched to in the event of a disaster.

The Disaster Recovery Plan itself should be clear and concise and able to be understood at any level of knowledge. It might not be the people that have been planned on to carry out the recovery of systems, since a large disaster could potentially injure and take lives. The documentation should be readable by anyone and cover all the critical functions with the right level of detail [5]. Putting together a comprehensive plan is a difficult task, no matter what is done, it will be regarded as too simplistic by some, and other will see it as unnecessarily complex for their particular function or role.

Most importantly the plan provides an outline for staff that should fully define all expected protocols, procedures and clearly define the responsibilities of each team member involved. It should be a clear response set to minimize confusion and uncertainty in the event of a crisis or disaster [6]. When staff and personnel know exactly what is expected of them, and it has been clearly defined the roles that each will take, it will lessen the fear and anxiety that naturally comes when responding to a disaster. It is not something they will have to guess or react to without a sense of purpose and knowledge that the plan is fully intact and covers all aspects of what needs to be done.

Contained within the plan should first be the definitions of disasters that the organization has agreed upon and what constitutes the implementation of the Disaster Recovery Plan.

. This will be different for every company as its dependencies on technology differ from one another. An incident can be categorized as a disaster if the organization is unable to contain or control the impact of an incident, or the level of damage or destruction from an incident is so severe that the organization cannot quickly recover from it [4]. The plan should define who has the right to declare a disaster for that particular company and when the timeline of recovery should begin. If the organization has a third party managed DR site, their contact information and procedure should be included at this point. They would need to be contacted and be prepared for the team’s arrival. Next it should include severity levels of disasters and what actions should be taken at each level. A company or municipality may have many remote sites and if taken out, may cause a level of disruption for business and serving the needs of the community, but may not constitute implementation of the entire Disaster Recovery Plan, only the systems or applications that reside at the remote location. The plan should then contain a list of necessary personnel and phone numbers in the order they should be contacted, the top of the list being the person responsible for initiating the Disaster Plan itself. This phone list should be given to all personnel on the Disaster Recovery Team and should be posted and readily available to all department contacts.

Next should be defined that Phases that are included in the recovery of critical systems. These phases should define the most critical systems being recovered in the first Phase with the appropriate Recovery Time Objectives. The number of phases is dependant on the organization and how many systems are deemed critical and need to be recovered for business to resume. Having phases also is a way of prioritizing systems and giving reasonable Recovery Time Objectives, also keeping in mind how long business will be conducted from the Disaster Recovery Site and when it can be either moved back to the original building or another site deemed appropriate by the Business Continuity Plan. If the disaster is something on a small scale that might only keep personnel out of the building for 30 days, only Phase 1 and possibly Phase 2 might be implemented depending on the number of systems that need to be recovered. The City of Raleigh’s critical applications were decided upon by an IRMC board. Hess says of the process, “The order of recovery was determined by the length of time each application would need and what function the application performed. The first decision was to insure that there would be continuity of the payroll systems for the employees. The remaining systems dealt with recovery applications such as GIS applications, inspections, public utilities, public works and so on. There are 18 critical applications in the city. The applications were recovered in phases until all were documented and tested.”

The document should be concluded with arguably one of the most important pieces, the instructions for recovering each system needed. This part of the documentation should be extremely clear and leave no room for mistakes or second guessing as the personnel recovering the systems may not be familiar with or even worked on these applications before. Nothing should be assumed about prior knowledge of these applications, while the best case scenario would be the personnel directly on the Disaster Recovery Team, the case

may be that personnel who have never worked on the system will be recovering it if no one else was available to leave. The documentation should flow in the same order that is expected to be recovered since some systems may require other services such as in a Microsoft Server environment Active Directory has to be fully functional before Microsoft Exchange email server can be installed and restored. This may seem like common knowledge to someone who works with these systems on a daily basis, but would be foreign to someone working with email for the very first time.

At the end of this document should be various forms that cover things such as documentation for the disaster. Just as with any other incident, although on a much larger scale, it should be carefully recorded from the beginning of the disaster. It could be vital in discovering how and why the disaster occurred if not of natural means. Also it gives a means of providing feedback and lessons learned from the disaster so that the plan can be updated and improved upon. Hess puts a lot of emphases on the after action reports. "The report which contains an in-depth analysis of the lessons learned is critical to our testing program. In addition, comments obtained from each DR testing person deployed to get their point of view on what happened. This is critical to the success of the program and the success of the people involved."

Overall the plan must be written in a way that procedures and processes can be switched instantly from one disaster scenario to another [7]. No matter how or what causes this incident to occur, the plan should be able to address any situation that arises and give clear direction on how and in what order systems should be recovered. There are many firms that could survive only a few days without computing facilities, this is why an effective and efficient disaster recovery policy or plan is a necessity that every organization should have [8].

III. TESTING THE PLAN

A key concern in the management of disaster recovery is that mistakes do not occur in the recovery phase [1]. A model in which the plan is tested and scenarios are run through gives a better sense of solidness to the plan and can point out areas that need to be improved upon, or changed for a smoother recovery. As in the case of the March 2000 Fort Worth Tornado, the reason given for such an effective response and recovery was steps taken to prepare personnel [9]. For several years prior to the tornado, the city departments had met and discussed scenarios and "what if" situations to prepare themselves and their personnel for an actual disastrous event. Preparedness reduces the "unknown" during a disaster and can even allow for enhanced flexibility in response [10]. Having a well prepared team can mean the difference between a fast and successful recovery of business operations, and a panicked and mistake filled attempt at recovery. When asked how he chose personnel to fill the disaster recovery team Hess responded, "I reviewed the skill set inventory for each person within the department. I then talked to each individual and ascertained their perception of the need for DR and availability to deploy.

I had to determine who would want to go and who would actually go. During a disaster, you cannot count on anyone, you must be several layers deep in your personnel choices and training. Without the right personnel, you will fail before you get to the site. The technical capabilities as well as the attitude of the person are critical. Without the right mix of these qualities, you will fail and that is a luxury we do not have in the DR world, to much is riding on the recovery."

It is important to have a strong team that is capable and resourceful, although the staff will not necessarily understand their roles unless they have been demonstrated and practiced with a well planned test [6]. If the staff have an opportunity to practice their roles they will more fully understand what is expected of them and be able to perform better under a stressful situation. A realistic disaster exercise is where the disaster recovery team will gain the most mileage and make the most impact in a number of areas. The procedures and steps will either be proven and work successfully or processes can be highlighted that may have worked out on paper, but need to be changed in a real life scenario. The exercise may also bring to light new and fresh ideas on solutions that might not have otherwise been known [6]. It is easier to think of real life solutions when you are in a situation rather than having to think up the problem and the solution on paper. A real life exercise creates awareness within the organization and can increase support and excitement for the project. Various other departments will want to get involved and see the need for the project when it has become high profile. This will also help with funding if needed, when the budget for Disaster Recovery can be split between departments rather than just becoming strictly an "IT project."

The test should be well planned and managed to not interfere and impact current business procedures and applications. Without the proper oversight the test could cause a real disruption of service if for instance the test environment was not carefully and meticulously safeguarded and kept off the production network. In this case, if budget allows, a disaster recovery test environment could be brought onsite to fully prepare. For smaller businesses this might be an adequate test of the plan, but it should be carefully watched to not allow "cheating" and using any tools and/or materials other than what has been carefully determined to be in the disaster recovery plan and would not be available in the event of a real disaster. For larger organizations who can afford offsite testing, an onsite disaster recovery lab could help prepare the team for the test, and ensure that the offsite test will be a success since it can be costly to send a team to a Disaster Recovery Facility and not have a successful test to show for it.

Tests and exercises are vital sources of feedback and short of experiencing a real disaster they are the only way of ensuring that the recovery plan will work. The lessons that are learned through these tests or exercises provide invaluable input into the planning process and ensure that the plan will not only work, but is fully understood and owned by the people who might one day have to use it [6]. The City of Raleigh has had four full tests. "The first two were unsuccessful" Hess states, "and the last two we have hit 100% of the Recovery Time Objectives. This has come about due to

the right makeup of the team, complete and vetted documentation, as well as Prior Proper Planning. Without these critical success factors, you will fail.”

IV. CONCLUSION

“If security is viewed as a core activity, it means a comprehensive emergency and disaster management planning framework and strategy will be in place, and a deep commitment to business continuity will be evident.[11]” The overall security of an organization is dependant upon its ability to quickly identify and properly manage a disaster should one occur. This will save money and prove to customers and citizens alike that the company or municipality is capable of handling and recovering from disastrous events. There are some cases in which having any plan at all is better than having no plan, but in the management of disaster recovery a haphazard and ill thought out plan can cause more confusion and mistakes. It is all about Prior Proper Planning, which equals Perfect Performance. Disaster Recovery is something that might not seem important until events happen that take out critical systems and there is no procedure in place to quickly get them back up and running. It is vital to an organization to see the importance of funding and fully supporting any disaster recovery effort that is undertaken because it ensures a long lasting effort the keep the company in business. It is a sad statistic that the majority of businesses still do not have a disaster recovery plan, and most businesses that fully loose their facility and data will not recover and go out of business.

REFERENCES

- [1] P. Trim, “Disaster Management and the role of the intelligence and security services,” *Disaster Prevention and Management*, vol. 12, March 2003, pp. 6-15.
- [2] E. Swartz, D. Elliott, B. Herbane, “Out of sight, out of mind: the limitations of traditional information system planning,” *Facilities*, vol. 13, Sept. 1995, pp. 15-21.
- [3] W. Burling, A. Hyle, “Disaster preparedness planning: policy and leadership issues,” *Disaster Prevention and Management*, vol. 6, Oct. 1997, pp. 234-244.
- [4] W. Lewis Jr., R. Watson, A. Pickren, “An empirical assessment of IT disaster risk,” *Communications of the ACM*, vol. 46, Sept. 2003, pp. 201-206.
- [5] M. Whitman, H. Mattord, *Management of Information Security*. Course Technology, 2004.
- [6] C. Maslen, “Testing the plan is more important than the plan itself,” *Information Management & Computer Security*, vol. 4, Aug. 1996, pp. 26-29.
- [7] P. Moore, “Critical elements of a disaster recovery and business/service continuity plan,” *Facilities*, vol. 13, Sept. 1995, pp. 22-27.
- [8] A. Kamsin, “Management of information technology: the study on strategy, planning and policies,” *ACM International Conference Proceeding Series*, vol. 90, 2004, pp. 152-157.
- [9] D. McEntire, “Coordinating multi-organizational responses to disaster: lessons from the March 28, 2000, Fort Worth tornado,” *Disaster Prevention and Management*, vol. 11, Dec. 2002, pp. 369-379.
- [10] D. McEntire, A. Myers, “Preparing communities for disasters: issues and processes for government readiness,” *Disaster Prevention and Management*, vol. 13, April 2004, pp. 140-152.
- [11] P. Trim, “Managing computer security issues: preventing and limiting future threats and disasters,” *Disaster Prevention and Management*, vol. 14, Sept. 2005, pp. 493-505.