Disaster Recovery

April 21, 2013

TABLE OF CONTENTS

INTRODUCTION **3**

PLANNING **3**

IMPACT AND RISK ASSESSMENT **6**

CONTROL MEASURES 8

TRAINING AND TESTING 11

REFERENCES 15

INTRODUCTION

Disaster Recovery is a process that aids organizations in planning for events that disrupt business; these events may be natural disasters such as flooding or fire, technical hazards such as power outages or software failures or human threats such as vandalism or terrorism (Guy & Lownes-Jackson, 2011). Organizations may not be able to plan for every possible disaster, but taking the time to develop a formal disaster recovery plan can prevent possible severe financial problems. An organization needs to focus on disaster recovery planning, impact and risk assessment, control measures, and training and testing when developing the disaster recovery plan that is right for the organization.

PLANNING

When planning for a disaster, you should look at all possible disasters that could be presented. It can be difficult to try and predict what type of disasters could arise, which is why everything should be considered (Burton, 2010). The first approach to disaster recovery planning is to identify critical IT resources by conducting a business impact analysis. A disaster recovery plan should also be created together with a business continuity plan. Identifying potential outages and allowable down times is also important. Developing recovery priorities can be crucial during the time of an outage. You have to set priorities within your group to clarify what to focus on. After the business impact analysis is completed, the organization should conduct a risk assessment of possible threats and vulnerabilities of critical activities and any supporting resources. Successful planning should include the understanding of a possible impact of an identified threat and how to handle any business downtime (Burton, 2010).

After the analysis and assessment is complete, it is important to look at recovery strategy and to create contingency plans. When creating a recovery strategy plan it is ideal to create different levels of impact for outages. An example of this could be an impact of 1, which would mean a minimal impact on one group or one user. An impact of 4 could be an entire site or group that is experiencing outage. Having this type of information well documented for employees will increase response time. Organizations should create a recovery team of responsible individuals to also increase response time. Having a high level team and an operator level team would be ideal for a disaster recovery plan. An example of a high level team member could be a manager or director. Your standard operator members could include one member from every group within your organization. This person would be the main contact for the group they are affiliated with. The high level disaster recovery group is normally the first to be informed and then they inform the operators who will then validate the severity level and proceed with the proper procedures.

There will be situations when a disaster recovery plan will need to be changed for various reasons within the organization. It is important that all documentation is updated correctly and reviewed by the appropriate people. The updated plan must be communicated with all internal and external organizations that would participate if the disaster recovery plan was implemented. All changes to the disaster recovery plan must be documented for future reference (Jessup & Valacich, 2008).

Most organizations have a detailed workflow of how an incident should be followed. An example of this could be that the incident is identified and a notification is sent out to the appropriate groups. After the notifications are sent out, business leaders will need to be updated with recovery strategies, impact assessments, and identifying critical and non-critical processes. After the recovery plan and restoration are completed and the incident has been resolved, it is good policy to have a set of post recovery procedures (Jessup & Valacich, 2008).

Post recovery procedures should be followed to determine if the system is ready to support the operation once again. Each group that is involved will need to complete their system checks such as patching, network, backup devices, core switches, access switches, and power systems. These are only a few examples and the checks will depend on the outage type and which groups are involved with the incident. Each group should have their own set of post procedures depending on the equipment that may be down (Panko, 2010).

Communication during a disaster recovery operation is vital for having a successful recovery plan. Employees need to have a clear line of communication to follow and have it on hand and easily accessible. The line of communication goes from the IT director to managers to team leaders, all the way down to support technicians. Names, phone numbers, position, and email should all be listed to increase response time. A well-documented list of disaster recovery team members should include their roles and responsibilities along with their contact information. It is very important that this document is up to date at all times. All members of the disaster recovery team should have a hard copy of the required documents. When an update does occur, that person should replace the old documents and dispose of them properly to avoid any security issues.

A successful disaster recovery plan eliminates or minimizes decisions that need to be made during a disaster. An organization also must have upper management support as well as the commitment from various groups assigned to disaster recovery (Panko, 2010). All possible disasters must be considered as well as all the needed recovery strategies to counter act these disasters.

IMPACT AND RISK ASSESSMENT

The process of performing an organization-wide assessment of any potential risk concerns and their underlying impact on systems, processes, and personnel is a very critical component of the disaster recovery process. Taking time to diligently analyze and assess the potential risks to the organization assists the process of ensuring that there is adequate preparation in the event of a disaster (Berthiaume, 2008). Possible risky occurrences can run the full gamut in terms of overall impact on infrastructure, product delivery postponements, and an inoperative customer service just to name a few. The possibilities are endless but the probabilities of particular events happening are higher in some cases than in others. This is why a high amount of importance is placed on the procedure of properly assessing risk levels in the case of a major or minor disaster, and making an intelligent determination as to what the specific impact would be on the organization as a whole.

There are multiple steps in the disaster recovery process; however, assessing risk and any resulting organizational impact is usually the first activity on the task list (Engle, 2010). In this way, all other activities that are of equal importance but require the detail within this assessment can be executed. As Godlewski (2010) emphasizes, a risk assessment will usually result in a prioritization of certain "critical processes" (p. 54) over others simply by virtue of them being of greater importance to the normal functioning of the organization. As such, it might be assumed that an occurrence that has a minor impact on a critical process would probably be considered of greater importance than an occurrence that has a major impact on a far less critical process. The aforementioned highlights the fact that it is necessary and important to consider potential incidents of risk while also placing an equal amount of importance on how critical the affected process, unit, or system is to normal business functions. In conjunction with the risk assessment and impact method described above, Pregmon (2007) recommends a "worst case scenario" (p. 23) approach in which a closer look is taken at the most terrible thing that could befall the organization and any of its processes. Utilizing this approach in some scenarios may be the most beneficial approach because the level of preparedness for all other risks or threats is high and the likelihood of recovering successfully is equally high.

Pregmon (2007) presents a logical step-by-step approach to the risk assessment and impact process of disaster recovery which includes the identification and description of risks, an evaluation of the probability that said risk will actually occur, and a description of the action plan that will be used to deal with the outcome of any risky situations (p. 23). Risks can come in all sorts of shapes and sizes but as was discussed in the previous paragraph, there is value in determining which activities are "mission critical" and whose absence could result in undesirable impact on the entire organization or business unit. Patel (2003) further reiterates the aforementioned steps in risk analysis and assessment by suggesting the importance of figuring out the probability that a specific risk will occur followed by a calculation of the impact on the organization in monetary terms (p. 46-47). This exact notion of probability and impact in monetary terms can be found in Pregmon' s (2007) formula for risk which is probability multiplied by loss, where probability refers to the "likelihood that a given event will occur" and loss is the entire *impact* of the risky situations that must be avoided, measured as a monetary value (p. 24). As such, the likelihood that a risky event will occur and the impact of its occurrence are positively correlated to one another. If a risk event has a high possibility of occurring and also has a meaningful impact on organizational technical and operational functionality for example, this is considered to be a high risk scenario, and should be considered a top priority in the disaster recovery process. Likewise, a lower likelihood of incidence paired with a minimal level of impact marks such an event low on the totem pole.

During the process of assessing risk and its impact on an organization's processes, infrastructure, and normal functioning, it is crucial that adequate preparation is made to evaluate the numerous scenarios that could possibly occur. The value added in prioritizing particular risk events over others is that the right amount of resources can be potentially directed towards those activities that are most vulnerable and as such, require a greater level of attention during a pending disaster situation. Even if resources are not put aside for a “worst case scenario”, there is no harm in being aware of all potential threats so that if the situation arises, there are sufficient measures in place to handle them.

CONTROL MEASURES

Control measures for disaster recovery are steps that can be taken to reduce threats or eliminate threats to computer security. There are three main types of control measures: preventive measures which look to prevent an event from occurring; detective measures which look to detect unwanted events; and corrective measures which look to correct and restore the systems after a disastrous event has occurred (Abram, 2012). Organizations must decide what control measures are necessary to put in place for their needs.   Disasters such as floods and earthquakes cannot be prevented; however, they can be prepared for. Once an organization lists and categorizes the possible threats that it could face, it can determine the impact of each threat. The cost of what steps the organization can take can be balanced against the tolerance for downtime that the organization is willing to withstand (Beaman & Albin, 2008).

Many experts would say that a disaster is a loss of data or perhaps system downtime that causes a loss of production. For computer systems, it’s important for the staff that is planning for disasters to look at the technologies currently in use and to determine what needs to be done in order to prevent or reduce downtime. These may include redundant hardware solutions like clustering or they may include companies that do mirroring backups or other types of backups that can be restored almost immediately. Planning also needs to look at what assets and business processes make up the operations of the organization. Critical operations are those that should be addressed when putting control measures in place. A Business Continuity Plan should be put into place to help avoid and/or mitigate risks. A BCP should look at: the risks of interrupting business operations, creating a plan to mitigate or reduce impact of those risks and what training is involved to that the plan will work as it was designed (Cerullo & Cerullo, 2004).

According to Guy and Lownes-Jackson (2011), to start, an organization needs to create and maintain an emergency contact list of its suppliers and have a plan for receiving services from those suppliers in the event of a disaster. It's important to know whether suppliers will support the organization at its location in the event of a disaster and whether the supplier is able to function in the event of a disaster at its location. Other businesses such as utility companies and landlords should be considered. Organizations also need to have a plan to notify employees regarding work expectations during and after a disaster takes place. If a disaster takes place during business hours, the organization will need to have an evacuation plan. An alternate site of business may be necessary to continue business operations. It is beneficial for business to coordinate efforts with local government if the disaster is community-wide; local governments may provide disaster information to the local businesses in their area. For technology, a remote site is needed with resources that duplicate what is used at the primary data center. High-bandwidth network connections should also be available. The best measures allow for redundancy of everything; this includes mainframes and servers (Beaman & Albin, 2008). Since loss of power is one of the most common causes of outages, organizations need to consider power supplies. Network connections must also be redundant and should follow different paths. Procedures should be defined and documented for: backups, safe storage of vital records, off-site storage, call notification, recover of systems/databases/applications, and remote operations.

According to Tipton (1997) examples of preventive controls include backups of files and documentation, fences, security guards, double door systems, locks and keys, backup power, biometric access controls, site selection and fire extinguishers. Preventive technical controls include access control software, antivirus software, library control systems, passwords, smart cards, and encryption. Preventive administrative controls include security awareness and training, separation of duties, procedures for recruiting and terminating employees, security policy and procedures, and supervision.

Examples of detective physical controls are motion detectors, smoke and fire detectors, closed-circuit television monitors, and sensors and alarms. Detective technical controls include audit trails and intrusion detection systems. Detective administrative controls include security reviews and audits, performance evaluations, required vacations, background investigations and rotation of duties.

Examples of corrective controls could include an operating system upgrade, backup data restore, anti-virus program installation or vulnerability mitigation. Experts have said that one of the most important aspects that are often overlooked is testing the control measures put in place to ensure they work as planned. Without testing, the organization is not able to guarantee that, in the event of a disaster, they will be able to continue necessary operations.

TRAINING AND TESTING

Both testing and training rely upon a major theme. This theme always comes back to management support and policy. Management is required to mandate rules and to support plans for testing and training. “The importance of planning for the eventuality of such losses is vital to limiting the amount of damage, decreasing the length of outages, and lowering the cost of recovery." (Southside, 2012) Testing is used to show to management and the employees that their procedures work. Training is required to ensure that management and employees know what and when to perform procedures to limit losses and damage.

Testing of a disaster plan ensures business continuity in that when a serious threat happens, the business will be well prepared. In an approach to testing, the responsible manager must direct the institution to prepare for testing using phases. "Recovery testing, whether soft or hard, involves four phases: test planning, test execution, establishing evaluation criteria and evaluating the results of the tests." (Molnar, 1984) When all of these phases are formerly documented, testing can then take place.

The document for testing disaster recovery planning is where all of the requirements are written down to procedurally test the disaster recovery plan. This is where the schedule of testing is recorded and assignments for employees are given. The document will describe the objectives of the test and how to grade the test. This document will also list employees and management roles.

The schedule for executing the test will come from the testing plan. It is important for the leader to follow the test plan exactly how it is written in the plan in order to find flaws in the documentation. Depending on the types of testing that take place, the tester can schedule and ensure responsible employees are available for the tests. "Some of the tests will include checklist tests, simulation tests, parallel tests, or full interruption tests". (Wold, 1997) Check list tests are basically check lists that are given to employees to ensure that the right employee is still working for the company and nothing of significant value has changed since the last checklist test. This will be a good time to make any changes and to re-instantiate the checklist test to those involved in the changes. Simulation tests can be full all out role playing sessions or used in smaller groups to ensure that the documentation of the testing plan is correct. Any faults with the documentation should be noted and sent through the appropriate channels for authorization and changes. Parallel tests are used to test the alternate site while the current site remains in operation. This allows normal operations to be conducted while testing is going on. A successful test gives management and employees confidence in the disaster plan. Also, any changes required can be addressed and updated. Full interruption tests actually interrupt normal operations and business operations are moved to the disaster recovery site that is covered in the plan. This test should only be conducted when there is reasonable faith that the plan will work and everyone is capable of restoring the original system, in case something goes wrong.

There are two final steps for creating valuable and accurate testing results. Establishing testing criteria is done to ensure that the plan works. This is where goals and requirements will be created. In this phase all tools needed for the testing processes are gathered and the knowledge to know what tools will be needed to create an accurate test are put into place. The final phase of testing is evaluating the results of the tests. "It is essential that the plan be thoroughly tested and evaluated on a regular basis (at least annually)". (Wold, 1997) Some of the important things to evaluate are the areas in the plan that needs to be changed.   If the plan doesn't work, then failures can happen that cannot be controlled. What really happens during this phase is that the plan gives confidence to management and employees, that when disaster strikes, the employees and management are competent to ensure business continuity.

Now that the plan works as expected, what happens when turnover and added functionality are created on the system? This can only be evaluated by more thorough testing of the plan and creating changes that will fix anomalies on the system. New employees must be trained and their roles in the disaster recovery plan must be integrated according to the plan.

Training is conducted as an overall security training program that is part of disaster recovery. There are two types of training that are available. One is formal training and the other is informal training. Both types of training are beneficial based on the needs of the recipient. “The purpose of disaster management courses is to create a group of educated individuals who are capable of handling almost any type of crisis that may arise in their home city, region, or country”. (WiseGeek, 2013)

In informal training, the recipient is provided knowledge that supplicants formal training, but is not part of any formal knowledge program. The recipient may have gotten training on databases, but does not have any knowledge of the current database schema.   The informal training on the institutions database schema is required to ensure accurate database restoration. Usually informal training is done in-house or by reading knowledge based materials by the employee.

Formal training benefits a large number of employees. This can be the most expensive type of training and may yield low returns if the employee is not motivated. Some of the more important parts of this training are that employees receive knowledge that creates layers upon preliminary knowledge that would let processes be produced to successfully complete the mission. The downside is that this knowledge will not crosswalk to the current systems and knowledgeable personnel must create informal training to complete the training process.

REFERENCES

Abram, B. (2012, June 14). 5 Tips to Build an Effective Disaster Recovery Plan. Retrieved from: http://www.smallbusinesscomputing.com/News/ITManagement/5-tips-to-build-an-effective-disaster-recovery-plan.html

Beaman, B. & Albin, B. (2008, June 25). Seven steps to disaster-recovery planning. Retrieved from http://www.smallbusinesscomputing.com/News/ITManagement/5-tips-to-build-an-effective-disaster-recovery-plan.html

Berthiaume, M. (2008, March). Is your business prepared for disaster? *New Hampshire Business Review*, *30*(6), 31. Retrieved April 21, 2013, from MasterFILE Premier.

Burton, C. (2010,). Disaster Recovery Journal. *The Death of All Hazards*, 23(3), 32-33.

Cerullo, V. & Cerullo, M. (2004, Summer). Business Continuity Planning: A Comprehensive Approach.

Engle, P. (2013, January). Making time for Strategic Planning. *Industrial Engineer, 45*(1), 18. Retrieved April 21, 2013, from Business Source Complete.

Godlewski, J. (2010, May). 7 Habits of Highly Resilient Organizations. *Financial Executive, 26*(4), 54-55. Retrieved April 21, 2013, from Business Source Complete.

Guy, R. & Lownes-Jackson, M. (2011). Business Continuity Strategies: An Assessment of Planning, Preparedness, Response and Recovery Activities for Emergency Disasters. Review of Management Innovation & Creativity, 4(9), 55-69

Jessup, L., & Valacich, J. (2008). *Information Systems Today* (3rd ed.). Upper Saddle River, NJ: Pearson Education, Inc.

Krause, M. & Tipton, H. (1997). Handbook of Information Security Management. Retrieved from: https://www.cccure.org/Documents/HISM/006-009.html

Molnar, Louie (1984). Disaster Recovery Testing, EDPACS: The EDP Audit, Control, and Security Newsletter, 12:5, 1-6

Panko, R. R. (2010). *Corporate Computer and Network Security* (2nd ed.) Upper Saddle River, NJ: Pearson Education, Inc.

Patel, R. (2003, October). Disaster Recovery Planning. *Automotive Industries*, *183*(10), 46-47. Retrieved April 21, 2013, from Business Source Complete.

Pregmon, M. (2003, October). IT Disaster Recovery: Are You Prepared and Ready? *Journal of the Quality Assurance Institute*, *183*(10), 26-27. Retrieved April 21, 2013, from Business Source Elite.

Southside (2012). IT Contingency Planning: IT Disaster Recovery Planning. Retrieved March 30, 2013 from: http://inside.southside.edu/security/documents/DDRandCOOPPlanTesting2012.pdf

WiseGeek (2013). WiseGeek: How do I choose the best management courses. Retrieved April 1, 2013 from: http://www.wisegeek.com/how-do-i-choose-the-best-disaster-management-courses.htm

Wold, Geoffrey H. (1997). Disaster Recovery Journal: Disaster Recovery Planning Process. Retrieved March 22, 2013 from http://www.drj.com/new2dr/w2_002.htm