GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

DESIGNING AND IMPLEMENTING A DISASTER RECOVERY PLAN

Goal

In the event of a disaster, be able to resume operation on an Application Server within the time determined by the Business Community.

Your Disaster Recovery Plan (DRP) should include the following documents:

1. DR Team Members and their contact numbers
2. Business Impact Assessment
3. Business Resumption Plan
4. Server/Network Documentation
5. Hardware and Software Support contracts and contact numbers
5. Backup Documentation
6. Restore Documentation

I. Build Disaster Recovery Team

A team needs to be assembled that will respond in the event of a disaster. This team should include a member or representative of Senior Management, members from the IS Department that will perform the assessment and recovery, representatives from Facilities, and members from the Business and User Communities to determine what level of recovery is needed and to verify that recovery is complete.

> "Crises, by nature, are generally complex and extremely dynamic. They leave only a small window of opportunity to do the right thing. Having your team in place is the most important step you can take to effectively manage a potential crisis."[1]

II. Determine/Evaluate Potential Sources of Outage

Identify potential sources of computer outages:

a) Hardware failure
b) Network failure
c) Software error
d) Malicious attack
e) Event that disables computer, computer room and/or site
f) Loss of personnel.

In most cases, a critical hardware failure can be repaired within a few hours, though this is dependent upon the level of support you have purchased from your hardware vendor. Your support level and substantiating vendor agreements should be included in your DRP.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The same is true if a network failure is caused by a hardware failure of your networking equipment. If however, the network failure is caused by a disruption in any way of phone service, the length of time to recover may not be knowable and will not be within your control.

Software error can be a user-mistake that causes bad or erroneous data to be committed to or deleted from a database. It can also be the application of a software patch that caused more harm than good.

Malicious attack can be any form of an attack with the goal of stopping your operation: malicious user error from inside; malicious hardware damage from inside or outside; malicious software damage from inside or outside; denial of service attacks, virus attacks, etc.

Severe weather, fires and explosions can destroy a computer room or building. Even if the room or building is not destroyed, these events can prevent users from accessing the computers by disrupting phone lines.

Although the computer and its applications are up and running, if all of your administrative personnel went to a conference and were victims of a plane crash, you have a disaster from which to recover.

III. Business Impact Assessment

Your Business Community must determine the time frame in which recovery from a disaster must be complete. The factors, which should go into this assessment, are:

a) Cost of the failure – loss of revenue;
b) Cost of recovery vs. loss of revenue;
c) Acceptable work-arounds during time of failure;

Datawarehouses may take a week or more to re-create, but they are generally not revenue producing. However, if you lost your order-entry or accounts receivable system, you will lose revenue until they are back on-line. Depending on the size of your business, you may be able to track orders and incoming revenue in spreadsheets for a week, but you still have to get that data back into the application once it is rebuilt. A decision must be made as to which applications are needed and when.

Once the allowable outage time has been determined, the feasibility and cost of the recovery must be determined. This is where you may be see the acceptable outage time go from 4 hours to 4 days.

Acceptable outages must be determined for each type of potential outage:

© SANS Institute 2000 - 2002, Author retains full rights.

a) Hardware failure – how long (and how much are you willing to pay) are you willing to be done due to a hardware failure?
b) Network failure – same issues as hardware failure.
c) Software error – if erroneous data was committed, weigh the time to manually fix the error (which may span many, many tables) vs. the loss of data if you recover your database to a point in time before the error was committed.
d) Malicious attack – you may not know everything that has been damaged, infected or removed by the attack. Determine if it is best to restore your software onto an alternate server until the original server is clean?
e) Disaster that destroys the server, computer room or building – you better have an alternate server at a different location;
f) Loss of administrative personnel – documentation will save you here.

The Massachusetts Institute of Technology has published its Disaster Recovery and Business Resumption Plans. They have categorized their business functions into 4 categories:

> **"Category I Critical** - must be restored to maintain as close to normal processing as possible [Maximum allowable down time 48 hours].
> **Category II Essential** - will be restored as soon as resources become available. [Maximum allowable down time 30 days].
> **Category III Necessary** - will be restored as soon as we return to a normal processing environment, data must be captured and saved for subsequent processing.
> **Category IV Desirable** - will be suspended for the duration of the emergency."[2]

Your DR Plan should include a similar assessment.

IV. Document the Server

You must document the creation and any major modifications to the Server. These documents must be written in plain English with the assumption that a person with a beginner's understanding of the operating system and any Applications can follow the steps to rebuild or restore the Applications. You should also document any patches applied and keep this list up-to-date.

V. Develop and Document Backup Plan

Determine the level and frequency of backups – daily full backups, weekly full backups with daily incremental or differential backups.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Send the backup tapes to an off-site facility for storage on a weekly basis. The time it takes to bring a tape back from off-site storage must be taken into account with assessing how long you will need to recover your system.

> "One alternative is electronic tape vaulting (ETV). This approach involves the use of a remote tape subsystem, typically located at a remote off-site storage or system recovery hotsite facility, as a destination for backup data sets generated by a company. In effect, the remote tape device is treated as a locally installed tape system. The difference is that the channel interconnecting the tape system to the host system is extended across a wide area network (WAN) link."[3]

The backup procedures must be documented, with step-by-step details on how the backups are done, when they are done, and what is backed up.

Most backup programs have the ability to log back up activity. Every time a back up is complete, the log of that activity is emailed to the system administrators. Include samples of these log files in your Backup Documentation.

Remember – you are not writing the document for yourself, but for someone who may not be familiar with your system and/or backup program.

VI. Develop and Test Recovery Plan

You must then test and document your recovery plan. You must perform various types of restores to be safe. Be sure to perform recovery from each kind of backup you do – full backup, incremental or differential.

To test a full system restore, you need another system. Restore from backup tapes from the production server onto your recovery server, being sure to document every step taken, the expected result, the achieved result and the time it took.

> "… documenting how testing is carried out, what issues are encountered, what the findings are, and what conclusions are reached is essential. Without records, tracking the status of the BCP is difficult or impossible. Furthermore, lack of documentation encumbers management decision-making and the audit process."[4]

These documents must be stored in multiple sites: on a shared hard drive that is backed up; hard copies in multiple storage cabinets in the office, computer room, and at the facility used for off-site storage of backup tapes.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

VII. Recovering from a Disaster

The above steps will help you recover from a hardware or software failure or user error. What about recovery from a malicious attack, where you may not know how much damage was done? Or how to get back in business if you lose your computer, your computer room, or an entire site?

One option is to have another server at another location. If you suffer a malicious attack you want to stop using the attacked server immediately to prevent the attack from spreading. You do not want to 'wipe it clean' and restore your files to it from tape. You want to get the computer off the network and let the appropriate investigative agencies take possession – whether these are internal security professionals or law enforcement. You want to leave the computer exactly as it is so that any evidence of the attack is preserved.

If you are fortunate, you will have a test/development server located at another site. This may generate network traffic between it and the production server, but in the event your production server is in any way lost, you can wipe out the test/development server and restore all production files to it. If you do not have a spare server, you can work with another company to be each other's DR site. There are also many disaster recovery companies that will provide this service.

Next, you must test this recovery. Again, the Business and User Communities need to be part of the test. Each step should be documented, including the time it took to accomplish each task.

a) A back up is done of the test/development server is done first. A time from which to recover is chosen, and the appropriate tapes are sent to the site of the test/development server or hot site location.
b) The test/development server is wiped clean and the production system is restored, from tape, onto the hotsite server.
c) The system and database administrators take a look at the system, the users are asked to log on and test. You need to test each process that is critical to running your business. Once they determine the test was successful this is documented and signed by management.

VIII. Maintaining Readiness

Now that you've documented your server, your backup and recovery steps, and tested them, you must be diligent in keeping your documentation up to date. If you change anything about how backups are done, document them. It is a good idea to develop self-audit checklists to document your diligence. Every time you do a restore, either because a user accidentally deleted a file, or because you are refreshing the database, document that action. Refer often to your instructional documents when performing these adhoc restores to make sure the

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

process hasn't changed. If it has changed, update the document. This constant documenting may seem tedious, but remember:

> "Maintenance of the plans is critical to the success of an actual recovery. The plans must reflect changes to the environments that are supported by the plans. It is critical that existing change management processes are revised to take recovery plan maintenance into account. In areas where change management does not exist, change management procedures will be recommended and implemented."[5]

If you are not asked to restore file(s) at least once a month, do so yourself. Move some files(s) to another location, delete them, and restore from tape.

You should schedule regular meetings of your DR Team, to keep everyone apprised of any new issues or concerns, and to keep everyone motivated and ready to recover your systems.

IX Words of Wisdom

Philip Jan Rothstein says it very well:

> "
> - Don't rely on top management's, clients' or other stakeholders' assumptions about your ability to deliver salvation from disruption – document explicit disaster recovery service level agreements which spell out the limitations as well as the promises.
> - Communicate regularly to stakeholders any technological, business or operational changes which impact disaster recoverability - don't wait until there is no longer a practical option or alternative, or until business management has already acted on the basis of out-of-date assumptions.
> - Present disaster recovery options, constraints and alternatives to business unit managers and to top management early in their decision cycles - don't wait until they are committed to a course of action which impairs disaster recoverability."[6]

---

[1] "Building Your Team For Crisis Communications" by Agnes Huff, PhD., found at http://www.disaster-resource.com. Click on Articles, then scroll down to "Crisis Communications & Response"

[2] "Critical Business Function Analysis Instructions", from MIT, found at http://web.mit.edu/security/www/critapp.htm

[3] "Backup to the Future: Beyond Traditional Data Backup" by Paul Carrick of Computerm Corporation, which can be found at http://www.contingencyplanning.com/article_index.cfm. Search for "Carrick" in the Author field.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

[4] "Does Your Plan Measure Up?" by Charles C. McKinney, found at http://contingencyplanning.com/article_index.cfm. Search for "McKinney" in the Author field.
[5] Disaster Recovery Planning – Project Plan Outline, by Computer & Networking Services, University of Toronto, found at http://www.utoronto.ca/security/drp.htm#DRP
[6] Managing Management: A Case Study, by Philip Jan Rothstein, found at http://www.rothstein.com/managing.html

© SANS Institute 2000 - 2002, Author retains full rights.