Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Disaster Recovery Plan Testing: Cycle the Plan, Plan the Cycle

Once a Disaster Recovery Plan (DRP) is created there is a tendency for management to relax. Disaster Recovery Journal, in an online poll conducted between May and June 2001, reported that 65.5% of 2223 respondents had not enacted their DRP in the past 10 years, and that a further 26.32% had enacted it only one to three times (DRJ surveys, 2001). These figures are astonishing considering that a ten-year time frame encompassed Y2K, several serious natural disaster events such as earthquakes and hurricanes and terrorist a...

Copyright SANS Institute
Author Retains Full Rights

AD

DISASTER RECOVERY PLAN TESTING, CYCLE THE PLAN - PLAN THE CYCLE

By Guy Witney Krocker

INTRODUCTION: ***"Quite simply, a plan which has not been tested cannot be assumed to work." (FIPS PUB 87)***

Once a Disaster Recovery Plan (DRP) is created there is a tendency for management to relax. "They feel comfortable and protected by the brand new, multi-volume set of emergency procedures sitting on a bookshelf in case of The Big One" (Haimowitz, Oct, 1996). Disaster Recovery Journal, in an online poll conducted between May and June 2001, reported that 65.5% of 2223 respondents had not enacted their DRP in the past 10 years, and that a further 26.32% had enacted it only one to three times (DRJ surveys, 2001). These figures are astonishing considering that a ten-year time frame encompassed Y2K, several serious natural disaster events such as earthquakes and hurricanes and terrorist activities such the World Trade Center (first attack) and the Oklahoma City bombings. Referring to DRP efficacy, Gartner Research states " a KPMG study shows that less that one half meet an acceptable portion of their recovery objectives" (Noakes-Fry & Diamond, Oct, 2001).

As a result of the September 11, 2001 attacks on the World Trade Center there has been a shift in priorities. "Back up plans and business continuity have moved up the priority list for many CIO's" (Cosgrove Ware, Nov, 2001) In CIO.com's October tech poll survey, 320 IT professionals were asked if the terrorist attacks of September 11 would cause their companies to change their disaster recovery plans, 54% said yes. In addition, 65% expect their IT contingency/disaster recovery spending to increase in 2002.

ACQUIRING MANAGEMENT BUY-IN: ***"…ten years from now, people may look back at 2001 as the year when disaster recovery shifted from 'a good idea when you can afford it' to 'integral to the heart of your business' ". (Rothstein, Nov 2001)***

Management buy-in is essential to the DRP process. The process of acquiring management support, commitment and funding may be as critical as any task in the entire process. Disaster Recovery Journal conducted an online poll between May and June 2001 that surveyed a total of 2151 respondents, when asked to describe the biggest challenge in planning efforts, 38.08% stated Funding, 32.64% stated Staff Shortage and 26.78 stated Complexity (DRJ surveys, 2001). Challenges associated with funding and staff shortages are directly related to the willingness of management to support the DRP testing process. Management willingness can be positively affected by the explanation of business impact, analysis outcomes and risk analysis results in terms they can understand and relate to. The factors that motivate management to commit to recovery testing are intrinsically linked to the factors driving the implementation of the DRP in the first place. Senior management must be made to understand that: 1) an untested DRP is unlikely to succeed in an actual recovery, and may in fact be more dangerous due to unverified assumptions; 2) the DRP is a dynamic document, testing and plan maintenance is an integral part of DRP development and implementation.

DETERMINING WHAT TO TEST:

In order to determine which business processes to test, the recovery practitioner must return to the core of the planning process. Each business-critical process defined in the DRP should be completely reassessed for currency and prioritized based on the Business Impact Analysis (BIA) and the Residual Risk (R_R) determined via Risk Analysis of threats, vulnerabilities and safeguards. Performing mandatory recovery

1) GIAC Certification Administrivia Version 2.0
2) Sans Security Essentials GSEC practical assignment version 1.2f

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

testing on processes with a high R_R and catastrophic BIA is a no-brainer and easily defensible to management. It is the less obvious values that will require management decisions as to what levels they deem acceptable. The recovery practitioner can simplify the process by implementing a ranking system in which the management can make decisions based on empirical data as opposed to subjective evaluations. The following ranking system is an adaptation of the methodology outlined by the Business Continuity Institute (BCI), London England.

Step 1: utilize the business process analysis performed in original DRP to isolate testable processes
Step 2: in conjunction with the process owner reassess BIA for each process; apply scoring from 0 to 5 based on increasing Impact
Step 3: in conjunction with the process owner reassess R_R for each process; apply scoring from 0 to 5 based on increasing Risk.
Step 4: matrixes BIA and R_R, in conjunction with management determine the testing threshold.

		R_R					
		0	1	2	3	4	5
BIA	0	0	1	2	3	4	5
	1	1	1	2	3	4	5
	2	2	2	2	3	4	5
	3	3	3	3	3	4	5
	4	4	4	4	4	4	5
	5	5	5	5	5	5	5

Fig. 1; Ranking matrices of Business Impact Analysis and Residual Risk
(shading denotes testing threshold)

In the example provided in Figure 1 a process with BIA score of three and a R_R score of 2 will be tested, a process with a BIA score of 2 and a R_R score of 2 will not.

The key to this method is that you have provided information based on current analysis with the process owner and have placed the responsibility on management to set the boundaries for testing.

SELECTING TESTING METHODOLOGIES:

Herein lies the theory versus reality interface. To this point we have, using industry best practices, provided a template for what needs to be tested and why. The challenge ahead is devising a testing methodology and implementation schedule such that;

- The DRP is tested to the fullest extent possible
- The associated costs are not prohibitive
- Service disruptions are minimal or non-existent
- The tests provide a high degree of assurance in recovery capability
- Evaluation of test results provides quality input to DRP maintenance

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

The Cycle Testing Paradigm:

Cycle testing consists of a series of exercises utilizing multiple methodologies that often increase in complexity and length from one phase to the next. The results of each test are assessed individually; improvements and error corrections are applied to the plan prior to beginning the next phase. At the end of the cycle the entire plan has been completely evaluated, in fact many portions of the plan will have been tested, assessed and updated multiple times. Small logistical errors that could prove to be major obstacles in full scale testing are isolated and removed from the plan. The opportunity to test-run multiple facets of a DRP with minimal costs and disruption to services and personnel in a low-pressure environment conducive to learning has incredible benefits. "Testing in cycles has a cumulative impact on the organization, infusing disaster recovery preparedness at all levels" (Hinds, 1994).

The iterative framework of the test cycle provides continuous DRP evolution. In the volatile world of Information Technology, hardware and software upgrades, configuration changes and even business process life cycling can occur quickly in response to market demands and new service requirements. Cyclic recovery tests provide an efficient pathway to DRP maintenance by early recognition and correction of such problems. At the end of each exercise and prior to the next, comprehensive debriefing, audit and analysis are required in order to update the current test plan as well as each of the following phases of the cycle.

Figure 2. Illustration of a DRP Cycle Testing Scenario

The test methodologies shown in Figure 2 are compiled and adapted from The Disaster Recovery Journal DR Glossary and from Testing Methods (Wold & Shriver, 1994). These methods provide a good fit to the Cyclic Testing Paradigm.

Checklist testing:

Without a doubt, checklists are the recovery practitioner's most valuable tools. They are inexpensive to implement and maintain and provide the backbone of the testing cycle. The checklists are team oriented and if used to their full potential provide multiple benefits.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

For each business process, partition out areas of responsibility, select teams appropriate to the specific nature of the partition and allow the cumulative experience of the group to develop the checklist as appropriate. The grassroots involvement heightens recovery awareness and buy-in as the team members get a sense that their input is an integral component of the process.

A checklist test can be used to validate multiple components of the DRP, for example:

- Emergency Call Tree verification
- Key procedure validation
- Hardware and software configuration documentation complete and current
- Availability of process specific resources during DRP implementation
- Tape backup libraries are complete and current with existing configuration
- Recovery plan and all necessary operational manuals

Walk Through Testing:

Team members verbally "walk through" the specific steps as documented in the plan to confirm effectiveness, identify gaps, bottlenecks or other weaknesses in the plan. Often used in conjunction with previously validated checklist plans. This test provides the opportunity review a plan with a larger subset of people allowing you to draw upon a correspondingly increased pool of knowledge and experiences. Staff will be familiarized with procedures, equipment and offsite facilities if required.

Simulation Testing:

A disaster is simulated so normal operations will not be interrupted. Hardware, software, personnel, communications, procedures, supplies and forms, documentation, transportation, utilities, and alternate site processing should be thoroughly tested in a simulation test. Extensive travel, moving equipment, and eliminating voice or data communications may not be practical or economically feasible during a simulated test. However, validated checklists can provide a reasonable level of assurance for many of these scenarios.

The simulation test should be considered advanced and only implemented after the previous checklist and walk through tests have been validated. Analyze the output of the previous tests carefully before the proposed simulation to ensure the lessons learned during the previous phases of the cycle have been applied.

Parallel testing:

A parallel test can be performed in conjunction with the checklist test or simulation test. Under this scenario, historical transactions such as the prior business day's transactions are processed against preceding day's backup files at the contingency processing site or hot site. All reports produced at the alternate site for the current business date should agree with those reports produced at the alternate processing site.

This test should be considered advanced and only be undertaken following due diligence with respect to the lessons learned from the previous phases of the cycle.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Full-interruption testing:

A full-interruption test activates the total disaster recovery plan. The test is likely to be costly and could disrupt normal operation, and therefore should be approached with caution. Again, the importance of due diligence with respect to previous phases of the cycle cannot be overstated.

There will always be surprises, unexpected results and alterations required from any recovery test. The ultimate goal is reducing the sources of error in the more advanced testing methods by effectively utilizing the relatively inexpensive Checklist and Walk Through testing procedures early in the cycle.

It is important to note that the test cycle can consist of one or more of the advanced testing methods. A Test Cycle should consist of a minimum of three phases, a Checklist, Walkthrough and at least one of the advanced testing methods. Figure 2 is an example of a testing scenario in which all of the previously discussed testing methodologies are employed.

SELECTING THE TEST TEAM: ***"The disaster recovery planning process is a splendid opportunity to provide common goals and to bring people from many sectors and levels of the organization into a positive collaboration"(Kabay, 1996)***

Planning stage:

The cycle planning team should consist of one or more individuals from each of the following departments:

- Management: continuous management input through the entire process is vital.
- Financial Dept: will assist in providing accurate cost analysis for each phase of the testing cycle.
- Legal Dept: can advise on contractual, regulatory and other legal implications.
- Personnel (HR) Dept: can advise on any issues involving contractors, Union implications or worker rights.
- Public Relations Dept: can advise on public opinion issues and responses to any outside enquiries.
- Security Dept: will ensure business and personnel security is maintained throughout the testing cycle.
- Process Owners: will provide the initial breakdown of logical sub-units for Checklist and Walk Through tests and provide realistic scenarios of process failures for Simulation or Full Interruption testing.

Testing Phase:

First line supervisors and their staff will be the people who actually carry out and perform the tests, additional personnel could include:

- Independent auditors
- Security staff
- Safety support staff

AUDITING THE CYCLE:

Each phase of the testing cycle is audited and analyzed for improvements, lessons learned are cumulative and brought forward from phase to phase. However, at the end of the Test Cycle it will be the Cycle as a whole that must be audited. The audit should consist of the following elements:

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- Awareness and training aspects
- Documentation Control
- Organizational and Administrative aspects
- Vital Records Security
- Structure, Contents and Actions of the Cycle as a whole
- DRP Maintenance procedures
- Contracts, SLA's or Other Commitments
- Suppliers Actions
- Logistics Flow
- Individual Test Phase effectiveness (success\failure)

CLOSING THE LOOP:

As we have discussed, each phase of the Test Cycle has provided valuable Lessons Learned and tangible input to DRP evolution. Prior to closing the book on the current Test Cycle it is incumbent upon the recovery practitioner to return to the results of each phase and ensure that all of the appropriate updates have been implemented in the DRP. Analysis of the flow and comprehensiveness of the test cycle should be conducted for primary input into the planning stage for the next DRP analysis.

In the assessment documentation you will prepare for management, there are several important issues that should be raised. Illustrate salient details of the changes to the DRP as a result of the Test Cycle in terms of lessons learned and if applicable, crises avoided should a real disaster have occurred rather than the test. The education of the entire organization in terms of recovery practice, procedure familiarization and increased comfort levels must be stressed. Costs associated with the Test Cycle should be compiled brought forward as a line item inclusion in the budget for the next fiscal year. There is no better time to secure funding for the next Test Cycle than when presenting the deliverables from the last. The high level of assurance you have provided management as a result of your successful DRP evaluation is a great asset in that regard.

SUMMARY

From a management perspective, the primary objective of Disaster Recovery Plan (DRP) testing is to evaluate whether or not the DRP is capable of restoring one or more business-critical processes to functionality within a specified period of time. At the end of the day a series of successful tests provides a high level of assurance for the business stakeholders, preferably with minimal associated costs and no disruption of services.

From the recovery practitioners' perspective, the audit and analysis of DRP testing provides key input into the maintenance of a functional DRP. Particularly in the IT world, a successful DRP is a highly dynamic document. Multiple input variables must be considered; hardware, software and business process life cycling, configuration management, recent regulatory and legal implications, risk analysis of newly identified threats, vulnerabilities and safeguards.

Cyclic, process based recovery testing provides a pathway to DRP maintenance and validation. A cyclic testing strategy employing multiple testing methodologies while increasing in complexity can provide adequate, cost-effective assessment for all input variables with minimal service disruption.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

References:

"Business Guide to Continuity Management" BCI
URL: http://www.bgcm.co.uk/guidance/BGCM%20Guideline.doc (February 25, 2002)

Cosgrove Ware, Lorraine. "IT Budgets Stabilize, CIOs Focus on IT Contingency Plans." November 1, 2001
URL: http://www.cio.com/online/110101_techpoll.html (February 25, 2002)

Disaster Recovery Journal current surveys.
URL: http://www.drj.com/surveys/robpoll/drj_surveys.htm (February 25, 2002)

Disaster Recovery Journal glossary
URL: http://www.drj.com/glossary/glossleft.htm (February 25, 2002)

"Guidelines for ADP Contingency Planning." Federal Information Processing Standards Publication. (FIPS Pub 87) March 27, 1981.
URL: http://csrc.nist.gov/publications/fips/fips87/fips87.pdf

Haimowitz, Mark. "Testings' the Plan." October 1996.
URL: http://www.contingencyplanning.com/article_index.cfm?article=54

Hinds, Judith. "Disaster Recovery Testing Cycles." Disaster Recovery Testing, Exercising Your Contingency Plan. Editor Philip Jan Rothstein. New York. Rothstein Associates Inc. 1994. 175-179.

Kabay, M. E. Ph.D. "Disaster Recovery Planning Encourages Better Managerial Decisions." ICSA Whitepapers. 1996.
URL:
http://www.trusecure.com/html/tspub/whitepapers/drp_encourage_mgmt_decisions.pdf

Noakes-Fry, Kristen; Diamond, Trude. "Business Continuity and Disaster Recovery Planning and Management: Perspective." Gartner Group. October 8, 2001.
URL: http://www.availability.com/resource/pdfs/DPRO-100862.pdf

Rothstein, Philip Jan. "Disaster Recovery. Sept. 11 changes everything." November 2001.
URL: http://www.infosecuritymag.com/articles/november01/industry_disaster.shtml (February 27, 2002)

Wold, Geoffery H.; Shriver, Robert F. "Testing Methods." Disaster Recovery Testing, Exercising Your Contingency Plan. Editor Philip Jan Rothstein. New York. Rothstein Associates Inc. 1994. 141-153.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**