A Brief Overview of the Disaster Recovery Planning Process

By

Jon William Toigo
CEO and Managing Partner
Toigo Partners International LLC
Chairman and Founder
Data Management Institute LLC

1538 Patricia Avenue
Dunedin, Florida 34698 USA
+1.727.736.5367
jtoigo@toigopartners.com

Executive Summary

Contrary to what you may read in the trade press, there is no "secret methodology" for developing a testable disaster recovery or business continuity plan. The activities involved mirror the structure of any complex development project. Common sense and business savvy are just as important as technical expertise.

This document provides an overview of the key steps of the planning process and offers suggestions on data protection technologies that planners may wish to consider to protect their most irreplaceable non-human asset: data.

Introduction

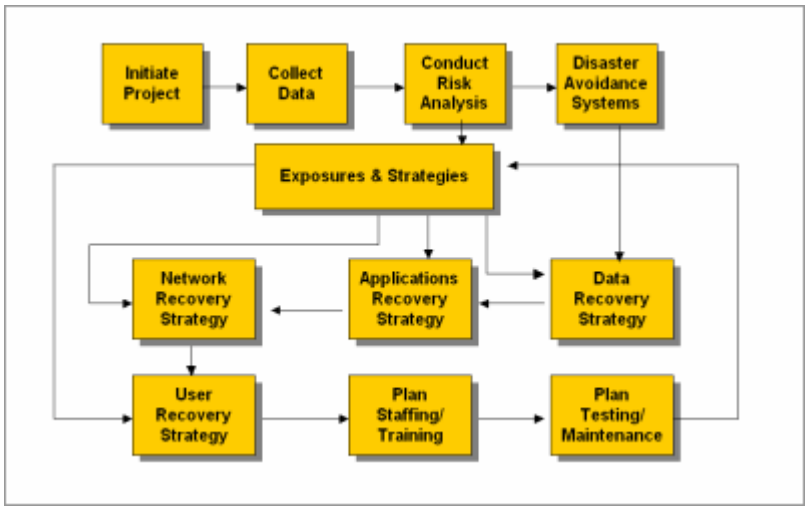
Disaster recovery planning has become a war cry in many organizations as the result of both the high profile media coverage afforded to recent natural and man-made disasters and increasingly strict regulations and laws mandating the protection and long-term retention of data -- an organization's most irreplaceable asset second only to skilled personnel.

Following is an in-depth treatment of what's involved in disaster recovery planning from a practical standpoint. The development of a DR capability is presented as a series of three discrete phases, each comprising a number of activities that must be completed in order to create strategies and logistics that may be submitted to testing.

For those who have not previously worked on a planning project, it is hoped that this document will help dispel the myths and help you focus on what needs to be done to develop an effective recovery capability.

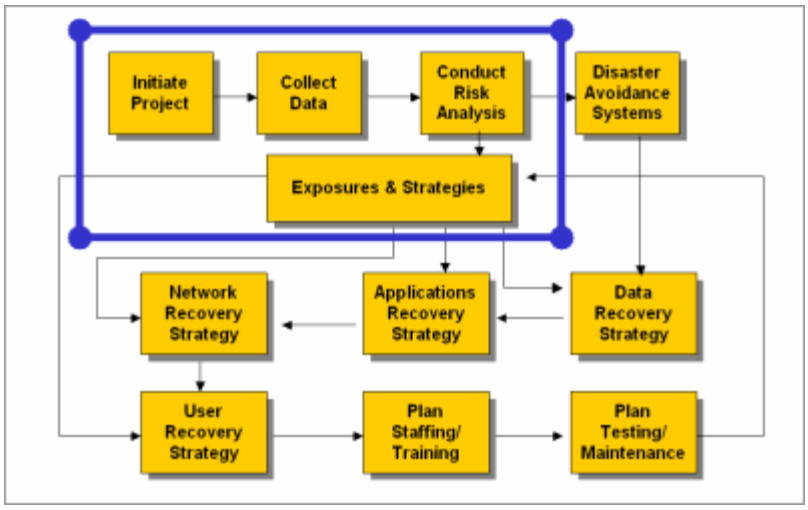
Phase 1: Data Collection and Risk Assessment

DR planning methodologies are often branded to specific consulting practices and represented as complex and convoluted processes known only to a few privileged practitioners. But in fact, the DR planning methodology is a straightforward application of common sense that follows a pragmatic project plan similar to systems development lifecycle methodology.



As shown in this diagram, the initial DR planning project involves 10 tasks, and these may be further refined into three subsets or phases. The first phase may be referred to as "Data Collection and Risk Assessment."

As shown in the next figure and discussed below, the tasks in this phase include project initiation, data collection and the completion of a preliminary risk analysis. Subsequent phases are "design," in which the capabilities are created to actually recover from a disaster, and "implementation," in which the strategies selected for recovery are tested and tests provide feedback to the planning process. This section will focus on the first phase and subsequent sections on the remaining phases of the planning process.



The disaster recovery planning project typically begins with project initiation. This airy task includes the assembling of a project team, possibly including internal and external subject matter experts, and the formulation of plan objectives, budget and other logistical matters.

One thing you should consider doing early is standardizing upon software tools for planning team members to use in collecting and assembling data. There are numerous DR templates available in print and as software that you may wish to consider to help standardize data collection, but desktop productivity software such as e-mail, word processing and spreadsheet or manageable database tools work just as well. The point is to have everyone submitting documents that are in the same format for ease of consolidation and analysis later on.

Data collection, the next task, involves the collection of information on internal applications and infrastructure, as well as the collection of information on risks and exposures drawn from various media, and the assembly of case study data on the disaster avoidance and recovery techniques used by other companies. Data is often collected and categorized into a "data store" or central reference repository, where those involved in later tasks can access it more readily.

Data collection aims at identifying business processes and the applications and infrastructure used to support them. You will also want to collect information about the cost to the organization of an outage affecting each business process that is 24, 48 and 72 hours in length. Interview department or business unit managers to obtain the costs both in terms of hard dollars and in terms of intangible losses (consumer confidence, etc.).

Following data collection and classification, the next task is risk analysis. Risk analysis involves the assignment of recovery priorities among business processes and the applications and infrastructures that support them. Partly, it is an attempt to predict the loss exposure of the company to interruptions of applications. Based on factors

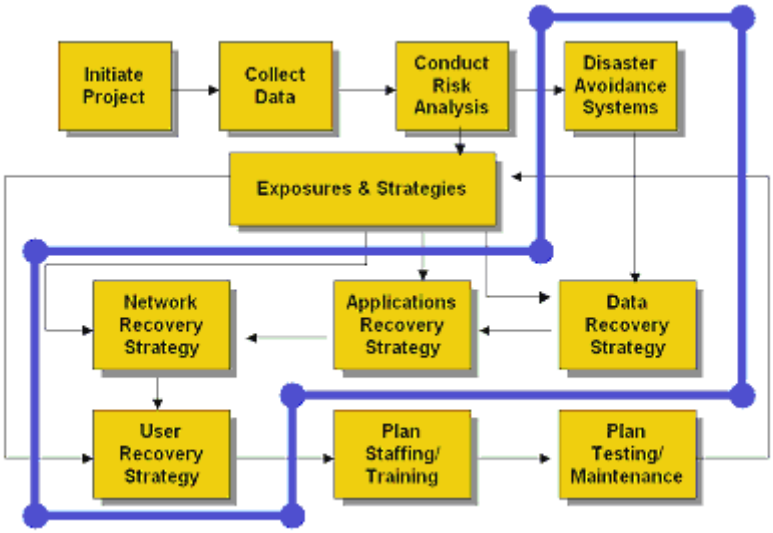
such as the accrued dollar loss exposure of an interruption event, criticality is assigned to each business process and to its related applications and infrastructure.

The "exposure scenario" that will guide plan development is also formulated at this juncture. Ideally, the scenario guiding a contemporary plan will be one of total loss of primary facilities, an aggregation of all dollar costs and intangible exposures accrued in 24, 48 and 72 hours following a disaster. This makes a compelling case for plan funding that may be important later if management commitment begins to wane. Ultimately, the plan you create should address the worst-case scenario but should be structured in a modular fashion to provide the means to respond to lesser disasters in a flexible way.

At the completion of the first phase, planners then turn their attention to the nuts and bolts of the plan: strategies for building avoidance and fault tolerance into their current environments and logistics for recovering data, application hosting platforms, networks and end-user work areas in the wake of a disaster. The philosophy that should guide this undertaking is simply stated, "eliminate disaster potentials that can be eliminated, and plan to minimize the impact of potentials that cannot be eliminated."

Phase 2: Design

Most of the tasks in the design phase (see below graphic) involve the development of strategies and logistics for restoring infrastructure and recovering data required by mission-critical applications in the wake of an interruption event. Each task requires you to consider multiple alternatives so that you can arrive at the strategy most effective within the constraints imposed by budget.



If a strategy entails a high cost, you should expect to have to justify its expense to senior management. Thus, wherever possible, seek strategies that offer "dual-use" value: Strategies that not only cope with disaster exposures but also deliver value to the organization in its day-to-day operations.

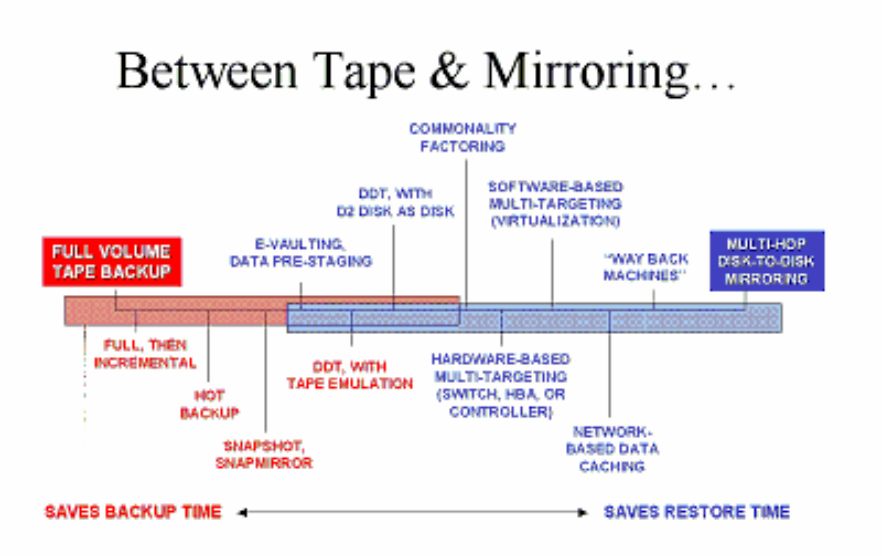
For example, consolidating storage into a fabric to share a tape library may afford better data protection than what is currently provided. But, it is a pricey fix. Discover what other value might accrue from the new topology, such as server consolidation and software licensing cost reduction, or the prolonging of the useful life of legacy tape silos, etc. The more robust the business case, the more likely your strategy is to get the nod from senior management.

People often ask which of the design tasks should be given priority if you are doing a DR plan on a budget. The answer is two-fold: Disaster avoidance systems selection and data recovery strategy development.

The disaster avoidance system task focuses on the deployment of technologies that help to identify conditions or events that could develop into disasters so they can be dealt with before causing interruptions. Avoidance systems (including management software, security controls, fire detection and suppression systems, etc.) not only prevent avoidable disasters, they may also help to save the lives of personnel.

Data recovery planning is the other task that must be viewed as among the most important. Unlike networks, systems and user work areas, which avail themselves of recovery strategies based either on redundancy or replacement, data protection is effectively limited to a single strategy: redundancy. To be safeguarded from loss or corruption, data must be replicated.

The approach selected for data redundancy typically falls somewhere on a spectrum between disk-to-tape (backup) and disk-to-disk (mirroring). A growing number of options -- once presented by the storage industry as an either/or solution set -- are now appearing between these alternatives. The figure below provides a current spectrum of data protection solutions organized by objective (time-to-backup versus time-to-restore).



In this spectrum, you can see the broad range of solutions that the storage industry has proffered in recent years to address the issues of time and cost in data protection.

To shorten backup times, various software features have been introduced, such as that supporting incremental backups, hot backups, inode snapshots, electronic vaulting and disk-to-disk functionality that emulates tape. Conversely, other technologies have been suggested to reduce the price tag of multi-hop, disk-to-disk mirroring. Some examples of these include disk-to-disk replication, data compression, software and hardware-based write replication schemes, and network-based caching.

So, there are many alternatives to fit many environments and budgets, and a lot of options for planners to consider.

How important is factoring in data protection in disaster recovery planning? Increasingly, one sees the metric "time-to-data" used to evaluate recovery strategies. This metric describes the amount of time required post-disaster to restore data access

to mission-critical applications and decision-makers. Time is money, and time-to-data is a measurement of the cost that will accrue to a disaster.

If companies have limited funds for DR planning, they are best spent on a combination of disaster avoidance and data protection.

This is not to minimize the importance of planning for application (and host platform), network or end user recovery. The more logistics that can be put into place to cover these important infrastructure components, the better.

However, many companies have found that, even when carefully defined system, network and user work area recovery schemes fall prey to the unplanned consequences of a disaster event, recovery of these elements can often be accomplished "on the fly." Data, however, cannot be replaced if it has not been duplicated in advance of a disaster.

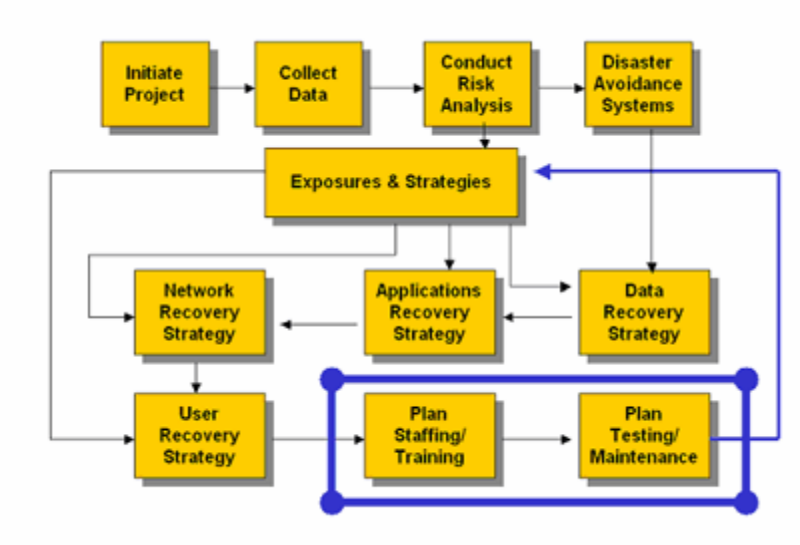
After all of the strategies have been designed and documented, the final phase (phase 3) of the planning project involves:

- The creation of recovery teams and their training
- Testing of the plan
- Implementation of a change management process

For the final point, above, implementing a change management process will capture test results and provide a "360-degree feedback loop" to the data store created earlier. This allows the plan to be reiterated and kept up to date with changes in the business and in its IT infrastructure.

Phase 3: Implementation

At this point, the lion's share of the work involved in defining recovery capability requirements and identifying strategies that will comprise the recovery capability has been completed. Contracts may have been signed with a hot site vendor, or a homegrown backup data center and user work area has been outfitted with the necessary computing, networking and storage infrastructure, to carry you through a facility-wide shutdown. More importantly, data copies are now being completed and verified as a matter of routine.



However, for all of the planner's hard work, the tasks that remain to be completed are among the most important in the planning project. For one thing, they ensure that the DR capability can be activated and used when necessary. For another, they create a constant process for capability improvement and enable organizations to ensure that their recovery capability is synchronized with their requirements.

The implementation phase involves the drafting of a plan document, or at least a decision-making flowchart that will walk a business or technical manager through the steps that must be taken in immediate response to an emergency. Note that DR plans are original and specialized for every company: there is no such thing as a useful boilerplate plan. Every plan is unique. The best are succinct and provide less detailed descriptions of tasks than one might suspect. That's because the paper plan is almost never referenced in an actual emergency. Moreover, it is not a script to disaster recovery, because disasters have a way of being a lot messier than planners ever anticipated when writing the scenario on which their plan is based.

Why go to the trouble of doing a paper plan (or an electronic one) at all? It's a good question. The answer is that the DR plan document is intended less as a script for recovery than as a training guide and testing manual.

After developing the disaster recovery capability, planners should carefully document "what needs to happen when" – the interrelationships and interdependencies between recovery steps – so that those who will likely play a role in recovery can be made aware of what their roles will entail.

There are no solid guidelines on how many teams a company will need or how many people need to be part of those teams. Common sense is the planner's best guide. A good strategy is to ask business unit or departmental managers who they believe would need to be involved in a recovery effort: select that person and a backup. IT will clearly need to have a significant presence.

Training consists of presenting strategies and procedures in a classroom environment. Train teams in what they will need to do in an emergency, but also provide sufficient context so they can understand how their work will impact or be impacted by the work of other teams. Take their feedback to heart, as they might identify requirements that you have overlooked.

Teams are also involved in testing, which is as much a training exercise as it is a rehearsal of plan activation. There are many ways to test and entire books written about the subject by DR planning consultants. Many planners prefer non-disruptive testing -- that is, tests that do not interfere with actual day-to-day operations. Testing by unplugging a server from power or from its storage is almost certain to bring about a career disaster.

One non-disruptive testing strategy is a walkthrough. Teams are brought into a common environment and a scenario is set forth. Then teams identify what they will need to do and speculate about the possible obstacles they may face and what may be needed to surmount them in terms of resources or time. Document the entire process.

Another strategy is to utilize the testing time that the company is granted are granted when it subscribes to a commercial recovery facility or hot site. Try to recover critical data and system and network operations and ensure that the necessary resources are available and allotted time is sufficient. The outcome of this test should be documented as well since it provides direct feedback on the continuing efficacy of the plan and identifies where the plan may have fallen out of synchronization with changes in business processes or IT infrastructure that occur on an almost daily basis.

Keep in mind that there is no pride of authorship in disaster recovery planning, just as there are no failed tests. Planners must keep the plan up-to-date and that activity involves both a testing regimen and a change management system. The latter may be as simple as a system of email notifications that will be made to the planner when team members leave the company or change jobs, when new business units are formed or existing business units change procedures, and of course when IT changes infrastructure.

Testing, training and change management are where the proverbial rubber meets the road in DR planning. In addition to all of the value of these activities described above, they also provide a mental rehearsal that will aid personnel in responding rationally in the face of the great irrationality that is a disaster.

As Shakespeare once wrote, "All things are ready if our minds be so."

The *Data Protection Strategy* series is published on an occasional basis by Toigo Partners International. Members of TPI communities, IT-Sense.org and Data Management Institute.org, receive a substantial discount on these reports and other informational and educational products offered by Toigo Partners International.

To find out about joining IT-Sense or the Data Management Institute, please contact us by email or visit the web sites at:

www.it-sense.org

www.datainstitute.org

