Practical DR
Realistic, achievable disaster recovery for your enterprise.

Practical Disaster Recovery:
A Cost-Effective Methodology for Business Resilience on a Budget

By Richard Rothschild & Doug Meier
Managing Partners, Practical Disaster Recovery, LLC
Saratoga, CA 95070
408.605.4832
consult@bcmastery.com | www.practicaldr.com

Executive Summary

If you can afford to hire high-priced consultants to set up and maintain a comprehensive, enterprise-wide BCP/DR program, stop reading now. This white paper is probably not for you. But if you're trying to implement Disaster Recovery on an ever-tightening budget, read on.

This white paper challenges the conventional wisdom that DR has to be an expensive undertaking. It clears up common misconceptions about what it takes to run a successful DR program. Many of these misconceptions come from "DR As a Service" (DRAaS) providers telling "total DR solution" fairy tales to IT managers tasked by executive staff with implementing DR in the short term.

In our experience, the pressure to implement DR in one fell swoop pushes organizations into wishful thinking mode, where they are susceptible to unrealistic promises of total DR solution providers. Just as there is no one-size-fits-all enterprise, there is no one-size-fits-all DR solution that will work over time. If you want a solution that begins with a DR consultant, there are plenty out there. A support agreement with a DR solution vendor does not mean you will respond adequately in a crisis, it only means that you've contributed to the DR vendor's recurring revenue model.

Organizations with DR mandates need to understand that every enterprise has a good amount of DR already in place. They simply need to focus on discovering and refining the DR that exists. There are mavens and connectors in the organization with the knowledge to fulfill the DR mandate, but lacking a pragmatic approach to implement DR. When the knowledge and the pragmatic approach come together, tangible evidence of real business resilience soon falls into place.

The Practical DR methodology described in this white paper encourages an incremental approach focusing on the most critical business functions and leveraging existing resource and processes. We advocate an ongoing DR strategy that parallels the enterprise's most significant initiatives, that is based on standard, good IT processes used to steadily build DR into the organizational culture.

A DR mandate does not have to be an additional cost burden. Quite the opposite: a systematic, build-it-yourself DR program that has executive support will reduce operational costs over time. There are things you can do right now – without a team of software consultants bearing templatized DR solutions – to build resilience into your business at very little cost.

The One Template Fits All Myth

Unfortunately, you can't buy DR off the shelf, install it, walk away, and expect it to run itself. DR doesn't work that way. DR works as an ongoing business resiliency process integrated with other business processes.

No matter how much money you spend on an off-the-shelf solution, you can't buy your way to business resilience. SunGard templates can get you started, but they won't finish the job. Any organization's DR requirements and implementation are unique. How can you expect a third party to understand the nuances of your enterprise when only your staff knows how your services run? It may be disappointing to learn that purchasing a set of DR templates doesn't give you DR, but by accepting this reality at the outset, you'll be more resilient in the long run.

It would be nice if you could write a detailed DR plan, assign tasks to team members, manage the project list for a few months, make the appropriate announcements, and then cross DR off the "to do" list. Flip a switch; it's done. Nice thought. But a successful DR program requires ongoing leadership, scope, and definition. Successful DR programs are proven through the committed involvement of key technical personnel in the organization.

Now that we've brought you down somewhat with a DR reality check, here's the good news: Quite likely the response and recovery processes the company has in place that can be leveraged to mitigate risk exposures, and at little or no cost. (Stop right here and visit the Department of Homeland Security's *Ready Business Mentoring Initiative*, which provides checklists of affordable (or no-cost) risk mitigations that can implemented almost immediately to protect the business.) The DR in place can most likely be leveraged now to implement a functional DR program providing true business resilience to your critical applications and services. An officially defined BCP/DR project or project budget is nice to have, but it's not absolutely essential.

And here's more good news: Once you've made DR part of your corporate culture, you can maintain it going forward without additional resources by integrating it into your existing processes. At successful companies, more often than not DR is an integral component of good standard business process. And here's even more good news: a well thought out DR implementation can significantly reduce expenses. Rather than adding cost, a solid DR program reduces operational costs over time.

Sideways on the Top-Down Approach

We don't dismiss the benefits of a top-down BCP/DR program. DR planning is a useful exercise in and of itself. But no amount of planning, awareness-raising, or internal communications can lead to true business resilience.

The following statement may seem counterintuitive, but it's true nonetheless: in the event of an actual disaster, the first thing that can be jettisoned is the DR plan. In a recovery scenario, people are either prepared to respond, or not prepared to respond. The idea of people rising to superhuman levels to recover from system disasters does happen routinely on TV, but not in reality.

Let's take, for example, a DR scenario from the popular American television series, The Office. Dwight Shrute, the mythical chief safety officer at Dunder Mifflin, in the course of an unannounced fire safety drill, screams at his co-workers to "use your adrenalin to sharpen your awareness!" -- which instruction only adds to the chaos. Michael Scott, Dwight's manager, shouts: "We're trapped! It's every man for himself!"

Our point is this: People can't rise to the occasion without being prepared to rise to the occasion. Successful recoveries don't happen just because a DR plan is in place. Getting to where people and processes are prepared to handle an incident appropriately is a result of small and medium steps taken over time. Beginning with the no-cost mitigations that can immediately build resilience into the enterprise at no cost.

This sideways approach isn't meant to discourage you from pursuing a top-down DR program, which can be a successful, systematic way to achieve business resilience. It's just meant to get you thinking that a DR program should support the organization, not be another cost center for the organization to support.

So where to begin? If nothing else, determine the DR that is already in place. This is the best way to determine what pieces need to be added, which in turn makes it easier to obtain required funding and executive support for DR.

The Discovery Process: Determining What Matters Most

Whether a DR project is officially approved or not, there are no-cost ways to reduce risk to critical business functions.

No DR consultant is required to identify a list of most critical apps and services. No DR planning folder is required to discuss how you would recover your critical services after a disaster. Taking both of these steps on your own may help prevent your company from going out of business.

Just identifying (or re-identifying) your top business risks is a useful exercise in preparedness. Deciding who is responsible for recovering which parts of the service is just another way of practicing survival skills.

Developing a document which details the order in which pieces of each service should be restarted (e.g. network, data bases, application servers, then web servers) is in itself a significant win. The relatively simple act of rounding up this information can lead to critical discoveries regarding

- systems, applications, and networks
- vendors, partners, and service providers
- policies, processes, and procedures

In almost all cases, the initial discovery process reveals exposures which can be immediately closed -- for instance, reliance on a single network interface, or tape backups that can't be recovered because tape heads are out of alignment (just to name two). The discovery process is a no-cost means of preventing potentially unrecoverable situations. With a little bit of effort, you are certain to reveal single points of failure, vendor non-compliance, servers without redundancy, services without reliable support, gaps in backup policies, bandwidth issues, capacity limits, and subject matter experts who have made themselves single points of failure by not documenting their critical knowledge.

Executive Sponsorship

According to conventional wisdom, executive sponsorship is the determining factor in any DR program. It's true that with executive buy-in, the road to DR can be much smoother. Executive buy-in is not absolutely necessary. There are plenty of practical, doable DR sub-projects that can be achieved on the cheap, without executive sponsorship. However, gaining executive sponsorship for your DR project is a worthy goal--one that should be approached strategically.

It's a commonly held belief in the DR community that the way to gain executive support is to raise executive paranoia of accountability and liability issues. There are plenty of documented cases where executives have been punished for neglect that led to massive loss in profits, customer confidence, reputation, and even the shuttering of the company. As reasons for DR, these are just scare tactics.

Executive support for DR doesn't come through liability scare tactics. They need toknow what's at stake. They need to know they can be resilient and reduce operational costs. The best approach to engage executive support for DR is to provide an initial scope of your DR program, including what is already in place. Separate the work that can be done at little or no additional cost from the additional work that requires executive buy-in.

In the final analysis, executive sponsorship for a DR program is dependent on one thing: executive perception of the DR project's positive ROI. Scare tactics focusing on executive "cost of ownership" are not as persuasive as awareness of potential cost benefit. If your project is truly dependent on executive sponsorship, then concentrate your energies on proving out the positive ROI.

Crisis Communication

In terms of DR, there is nothing simpler to achieve, or easier to improve, or more immediately beneficial, than the ability to communicate in a crisis.

- Leverage the escalation and notification paths in place. Refine them, update them, expand them.
- Define first, second, and third tier escalations for critical systems--so people outside the organization can escalate properly.
- Maintain and update the list of vendors and service providers who provide critical services.
- Formalize functional roles and responsibilities for critical applications and services. Make these part of overall performance objectives for individual team members.
- Develop and document an agreed-upon Disaster Declaration guideline. Focus on the ability to use RTO to quickly assess impact, duration, and spread, and determine whether an event is an outage or a real disaster.
- Test your primary and secondary DR team communication modes. If corporate email is down, communicate over chat or SMS. If HQ is inaccessible, arrange for an alternate physical site. If phone system is down, have a cellular call tree.
- Test your ability to get the right messages to the right people in a crisis.

Transforming inadequate crisis communications to responsive, appropriate escalations and notifications paths is perhaps the quickest, most cost-effective means of achieving a basic level of DR capability. If the right people are communicating with the right people, there is a good chance a crisis can be resolved adequately. If not…

There is literally no one in the world more capable of developing effective crisis communications than the staff tasked with responding. Developing crisis communication mechanisms requires little if any outside expertise -- only common sense, and an awareness, shared among team members, of the criticality of good communications in any service interruption event, large or small. These are the first steps in developing the critical "culture of DR" described later in this white paper.

Compliance, Data Protection, and Business Resilience

Service agreements, recovery testing, and monitoring are critical to achieving and maintaining business resilience. Ultimately, business resilience is gauged by the enterprise's ability to demonstrate that policies and processes are in place to protect and secure critical data. In this respect, compliance with regulatory standards and agencies goes hand and hand with DR.

Generally speaking, companies take one of two approaches to compliance: (a) lament the laws requiring regulatory compliance, and lobby Congress to rollback Sarbanes-Oxley, and do the work grudgingly anyway, or (b) look at compliance as a means to a greater end. The point being that organizations with a positive outlook to compliance view the effort required to demonstrate compliant data protection capability as a means to accelerate the pace of business.

Compliant data protection policies and processes, implemented and maintained with some rigor under the auspices of an ongoing DR program, can provide important data protection safeguards that would not otherwise be addressed. Just one example: The important legal distinction between what is an acceptable backup policy process and what is a data archiving requirement. In our experience, regulatory requirements for SOX, PCI, HIPPA, and SAS70 tend to compel businesses to distinguish data retention needs from data preservation needs. In this way, the annoying quarterly SOX audit provides a unique opportunity to establish a clear separation between when, where, and how data for normal operations is *retained* and when, where, and how data required for litigation, audits, or regulations is *preserved*.

If compliance is having standard, secure business processes and procedures in place, and people familiar with the appropriate response and recovery processes, then compliance is the same thing as DR. A good DR program addresses compliance, and compliance efforts in turn leverage the DR in place.

Data Classification

Data Classification is the single important step in the Disaster Recovery (DR) process. And it's also the most overlooked.

The process of identifying and categorizing the data most critical to your business, and the data that is not so important, will provide immediate and long-term benefits. Data classification, undertaken properly, will increase the manageability and reduce the scope and cost of your DR project.

To classify the data, set up a spreadhseet (or comparable tool) which lists the key services. Provide at least the following:

1. The level of importance to the business from 1 - 5
2. Who is responsible for running this service (e.g., System administrator or Network Engineer)
3. How much data is being stored today
4. What type of data is it (e.g., Oracle database, ERP, spreadsheets)
5. Any dependencies connected to this data

Collecting this information requires interviewing the mavens--the subject matter experts--who actually manage the data. The people who handle the data on a daily basis have the most knowledge about how it actually runs, along with the potential obstacles. This process can take weeks or longer to elicit and assemble for review but it is really the least effort in the long run.

Once data us collected from mavens and other subject matter experts, order it by relative importance. (You should be working from an agreed-upon definition of “criticality”.) Create tiers of data—for example, level 1 for most critical, 2 and 3 for less critical and not critical. A simple tiering exercise will reveals what to focus on and what not to focus on in the DR project.

Vendor Resilience

Perhaps the most overlooked aspect of DR is vendor resilience. Think of vendors in the broader sense, as any external entity that the organization does business with or relies on for supplies, services, and technology. Just as there are critical applications and services and processes that deserve the focus of a DR program, there are also critical vendors who warrant the same attention.

Regulatory requirements are putting more of the onus for vendor resilience on the service owner. Moving forward, it is more important for the corporate consumer to verify that a particular vendor has a truly secure, hardened setup. From a compliance point of view, it's up to the corporate consumer to prove due diligence in finding vendors with secure facilities, services, and survivability.

From a pragmatic, doable DR point of view, vendor resilience is about evaluating and fortifying the vendor list. Just the act of centralizing the vendor list to eliminate obsolete or unnecessary information is a worthwhile undertaking. Syncing Purchasing's list of vendors with the non-approved vendors used by individual organizations is always an illuminating exercise in information management.

The process of evaluating vendors is becoming more normal as is the process of evaluating a vendor's financial health. Using multiple or secondary vendors as an operations strategy is a means of testing the depth or robustness of your vendor list, a DR risk mitigation built into the organization's way of doing business.

Service Agreement Management

Service agreements are the ignored stepchild of most DR efforts. But they can be more than an afterthought. Service agreements, both internal and external, can be useful if part of a strategy of vendor, service provider, and partner resilience.

It's not an absolute necessity, but assessing the effectiveness Service Agreements in place does fall within the scope of a practical, results-focused DR program. For organizations taking on better Service Agreement management as part of the DR effort, the end result is "hardened" service agreements with meaningful language, appropriately monitoried and measured as part of a healthy business relationship.

You can't have a meaningful – and by "meaningful" we mean "truly useful and enforceable" -- Service Agreements without:

- Knowing precisely what you are most concerned with monitoring, or evaluating
- Establishing the monitoring requirements and parameters
- Establishing the metrics for evaluating the monitoring data provided

When these are included, the Service Agreement has a good chance of being useful working agreement between two parties, and sys admins receiving alerts in a DR scenario are more likely to appropriately engage with the support techs, service reps, consultants – whoever is on the other end of the phone call.

Here are some common areas of inconsistency found in most Service Agreements:

- SA not precise in ownership and accountability
- Separation of computational and communication infrastructure
- Inadequate identification of service points of presence
- Monitoring metric collection approaches not detailed
- Monitoring data reporting not detailed
- SA ownership unclear, unknown
- Violation detection and notification as part of SA oversight

Service Agreement management doesn't fall within the scope of a DR program, however assessing and evaluating Service Agreements in place does fall within scope, and can quickly lead to hardening the Service Agreements in place, a better standard for developing and monitoring new Service Agreements.

Reality of DR programs

In very few cases is DR implemented as an uninterrupted, beginning-to-end business solution. More often, DR is something that occurs in fits and starts over time, if it occurs at all. Why?

Because DR programs are neither easy to define nor implement. Because it's difficult to grasp DR in its entirety. Because DR encompasses all your business has built since it was formed. Because the benefits are not immediately obvious, or tangible. Because it seems like a very costly endeavor. Because there are lots of other fires burning and so far "the big one" hasn't happened. Because DR is not part of the corporate culture.

For all of these reasons, most DR programs languish after the planning stage, leaving the enterprise pretty much where it was before in terms of resilience; that is, just as unprotected as before the first DR project kickoff event.

Once implemented, DR has to be maintained. Like compliance audits, DR maintenance can be approached in two ways: as something for the organization to get past, or as something to make the organization better in the long run. In the second way, DR is more likely to be successful over time, and over time the DR program becomes an ongoing business process that is tested and adjusted to reflect changes to the business, including changges in the applications environment, data center environment, changes to the organization, changes to personnel, and changes to recovery processes and communication processes.

The DR program doesn't have to be perfect to succeed. There are going to be times when recovery processes or on-call lists aren't updated. There is going to be an application or service not being monitored adequately. There are going to be new people without adequate training in key processes. Fortunately, business resilience is not on all-or-none proposition. The value of a DR program can be demonstrated by exercising the people in established response and recovery processes. So the value of DR can be demonstrated at any time, not just during a real disaster event.

Benefits of a Practical, Realistic Approach

A practical, doable approach to DR gives the organization just what is needed to mitigate risks and ensure survival. This practical approach is in contrast to the resilience that "DR as a service" providers promise to deliver, in million-dollar increments. Renewal agreements with DR solution providers don't have lasting value because they don't work toward building DR into the culture.

Total vendor solutions to DR tend to overlook the tangible working understanding of the DR that an organization has already in place. They tend not to focus on risk mitigations that can be completed at little or no cost to improve the resilience of the most critical business functions.

The concept of addressing what can be done now, today, at little or no cost, using existing resources, is too often missing in DR programs. In particular, DR programs outsourced to a DR solution vendors as a result of a DR mandate that is not fully understood, tend to lean to the "DR has to cost an arm and a leg to be any good" philosophy. Outsourcing DR does not necessarily buy resiliency for the business functions that are most critical to the enterprise's survival. Not without expensive renewal agreements.

For organizations that can, we recommend a practical, self-sufficient approach that provides tangible results, sooner and lowers operational costs (instead of adding to them) over time. This approach is built on the following:

- involvement of key personnel
- focus on projects that matter most to the company
- documentation of key processes of who will do what in an incident
- close integration with compliance and regulatory efforts
- organizational awareness of who is responsible for what in the event disaster
- replacement of non resilient vendors and service providers with resilient vendors and service providers
- testing and auditing of response and recovery procedures built into standard operations

Culture of DR

A successful DR program has definite attributes.

- DR is instilled in the corporate culture, discussed in hallways and at the watercooler, debated over lunch
- DR requirements are automatically considered in new technology appraisals, in project requirements documents, at the start of new program initiatives
- DR is rolled into performance objectives, measured in performance reviews
- Business resiliency is required of internal and external partners

Weaving good standard Disaster Recovery practices into the fabric of your company is the best way to ensure your DR efforts continue, and the best way to guarantee that budget and resources will keep flowing into your DR project.

Instilling DR takes some effort, but it may be easier than you think. Your employees are by nature open to the concept of business resilience as it relates to the survival of the enterprise. The key is to incorporate DR into your business strategy -- your planning and your objective-setting -- *up front*, not as an after-thought. Much like earmark spending is considered when reviewing budgets in Congress, DR should be an allocation for businesses as well.

How to make this happen?

- To begin with, set up a weekly DR team meeting to specifically discuss DR
- Add DR as an agenda item for regular staff meetings
- Make DR part of your objectives, and an objective for those who work for you
- Insist (remind, plead, beg) that DR be included as part of the scoping for newly proposed projects
- Persuade your manager to include DR in her objectives
- Designate someone in your organization to become a Certified Business Continuity Professional (DRII provides basic course and advanced business continuity certification)
- Add pieces of DR to approved projects where it makes sense
- Incorporate parts of DR into various cost-cutting projects (yes, you can improve resilience while reducing expenses)

Your ability to instill DR into your culture is a major determinant of the success of your DR project. The more DR becomes part of normal business process, the higher the probability your DR project will succeed, and the lower the likelihood your company will be severely damaged by a disaster. Instilling DR into your corporate culture will not only help your company survive, in the long run it will make your company run more efficiently.

Conclusion

We've taken you through a practical, doable DR methodology that focuses on risk mitigations in place and no-cost to low-cost mitigations that can make the organization more resilient in the short term.

This is not a criticism of traditional business continuity programs, which are most effective when implemented as an uninterrupted end-to-end project that involves stakeholders across the organization and a strong business mandate from customers and the board of directors.

Unfortunately, DR isn't stamped out. It's usually built in fits and starts, over time. That's the reality of most DR programs.

Business resilience is as unique as the organization. Leveraging the knowledge and the means that the organization already has in place, merging that knowledge with a pragmatic approach that focuses on resilience of the most critical business functions, and focusing on demonstrating standard good response and recovery processes – this approach, this is the best means of building a culture of DR within the organization. And this in turn is the best means of providing business resilience over time.