Introduction to BCP and DR Planning

Based on the book RESPONSE! *Planning & Training for Emergency Recovery*

November 24, 2015

Tim Elemes
Huber Advisors
P.O. Box 175
Hugo, MN 55038
information@huberadvisors.com

Business Continuity Planning (BCP) and Disaster Recovery (DR) planning focus on preparing an organization to successfully preserve and recover business operations after a disrupting event.

How to tackle BCP/DR Planning

Business Continuity Planning (BCP) and Disaster Recovery (DR) planning focus on preparing an organization to successfully preserve and recover business operations after a disrupting event. The ability to recover depends entirely on thorough BCP and DR planning.

Preparing to deal with the aftermath of a disaster requires several steps:

1. Identify a location for carrying out critical business
2. Identify a location for IT to re-establish critical infrastructure and operations
3. Ensure the recoverability of data
4. Understand the process for re-connecting users to the recovered data
5. Train recovery teams for immediate action upon notification
6. Understand the decision making process during recovery proceedings
7. Plan for cash needs during recovery
8. Plan for the notification of clients, employees, regulators, stakeholders, and media
9. Plan for the actual recovery while

    - Protecting the good name of the company
    - Responding to media, regulators, investors, and employees
    - Counseling those caught in the disaster
    - Counseling those dealing with the stress associated with the recovery process
    - Managing contractual obligations under emergency conditions

All of these steps are focused on and in support of recovery of critical systems and services needed by the organization such that they can continue to produce their work product, support the existing client base, and ensure the overall livelihood of the organization.

Business implications

When generating recovery plans, minimizing the impact on the overall business is the primary objective. In other words, the plan must be such that critical systems and services have been identified, plans for their timely recovery are in place and well-understood, and those performing the recovery have been trained on their execution.

Identification of Critical Services provided by the business

There are multiple ways to approach identifying the critical systems and services on which your organization relies, and as a result, how much planning and investment is the appropriate amount for that service's recovery. There are a lot of different approaches and options for performing a Business Impact Analysis (BIA). Some can be quite costly, others quite voluminous, others simply inconclusive or at such a level of detail to be of questionable worth.

It is rare that an organization, as well as any functional area within an organization, is unable to clearly articulate the critical systems and services they need in order to meet the responsibilities of their functional area. Instead, more of a reasoned, almost discussion-based series of interviews has shown promise in identifying an organization's critical services and functions.

The first approach to consider is a Probability-based approach. This approach is based on having analysts multiply the potential loss experienced following a disaster by the probability of it occurring and then comparing that to the cost of backup alternatives.

For each system:

> The expected frequency of occurrence per annum, P, as well as the loss incurred, C, are calculated, and the exposure, E, per annum is then evaluated from the values of P and C. (E = P * C). The higher the value of E, the more resources should be allocated to address loss as it relates to this event occurrence.

If this is the sole approach for determining your planning strategy, the organization may be exposed to unacceptable losses when a very low probability disaster actually occurs.

Another method is what is sometimes termed the prudent person methodology. This approach is based on executives eliminating planning alternatives that risk the short and long term viability of the firm. From there, in-depth analysis is performed on the remaining alternative to select the lowest cost alternative that provides acceptable recovery times. Key to this approach is the assumption that officers of the company performed a reasonable investigation and honestly believe that their decision is in the best interest of the corporation.

A third way to look at the planning needs is an intuition-based executive approach. With this approach, a team is put together to use different evaluation criteria in order to ensure more perspective is brought to the decision. The table below gives an example of the different possible executive roles and their respective criteria:

Stakeholder	Evaluation Criteria
Executives	Assure continuity of a viable organization
User Management	Continue operations with minimum impact on user experience.
IS Management	Continue operations with minimum impact on system availability.
Auditors	Continue operations with minimum impact on financial viability
Financial Analysts	Minimize long term costs

Identifying the key risks

Regardless of the means for identifying the critical systems and services for your organization, it truly boils down to the management and mitigation of operational risk. Each organization will have its own set of risks and risk factors based on their environment, their industry, the level of regulation, and so on.

In Diagram-1 below, an example of the different areas and levels within an organization where risk is identified and plans, process, and procedures are put in place to address these risks.

Diagram-1: Risk Planning Continuum

The bottom-most section in blue, represents the risks associated with the IT infrastructure, systems, and services used throughout the organization. As depicted, the IT recoverability, and mitigation of operational risks with IT, truly does establish the foundation for all other planning. It does not necessarily mean that an organization MUST start with IT planning when looking at mitigation and management of risk; however, it is rare in today's business environment to find a business that hasn't already put a certain amount of time, talent, and dollars into IT recoverability. This does provide the means to build up the hierarchy, leveraging what is in place, as well as providing the means for identifying shortcomings in the implementation of IT solutions as compared to business needs.

As the organization's recover planning maturity increase, the topics identified in the red section become more prevalent. With the IT foundation in place, discussion now focuses on broader operational needs within the organization, and vetting of the IT solutions starts to take place. This is when terms such as Recovery Time Objective (RTO) and Recovery Point Objective (RPO) become important.

Without going into a long dissertation on what these two metrics represent, suffice it to say that understanding RTO and RPO allows organizations to more clearly articulate how quickly they need critical systems and services to recover after an incident, and to determine their ability to absorb aged or even lost data.

Here is an example of the impact of understanding RTO and RPO:

> An assessment was performed on a company where the key members of different business functions were asked the question: What would happen if IT was unavailable? Some key answers were:
>
> ***"…there's no way we can do it manually. We might as well go home…"***
>
> ***"…our productivity would drop by more the 60% without IT services…"***
>
> ***"…we could last maybe four hours without IT…"***
>
> The last statement is critical in determining the RTO value for the organization. The challenge was that when asking IT how long it would take them to recover, the answer was an estimate ranging from 22 to 28 hours.
>
> So – what do you do about the difference?
>
> Or perhaps more importantly, are all the key decisions makers aware of this gap, and is it acceptable to the business?

The key point here is that as organizations progress up the pyramid, there needs to be a process to ensure alignment from top to bottom. For instance, when getting to the top of the model, where policy statements come into play, ensuring that implementation to support the policy is crucial.

Take for instance the policy statement:

> *Our general recovery policy is that any IT system or service that supports revenue generating activity, and has a financial impact to the organization of more than $1500 per hour when unavailable, will have a means for full recovery in place in order to support a recovery time of no more than three hours from loss of said service.*

This type of statement starts at the top of the hierarchy, but true implementation of the statement would be in the bottom-most layer. If the solution does not meet the policy's requirement(s), it then needs to prompt action. To be clear, and in this example, it does not necessarily mean that the IT team did a poor job in putting together the solution. It could instead identify an area where more capital expenditure is needed in order to support organizational policy. The point is that the entire hierarchy of plans has to be aligned.

In some cases, risk assumption will come down to the point where an organization simply concludes the risk is one they are willing to accept rather than investing in new solutions to minimize or mitigate that risk – which in turn needs to prompt periodic review of insurance coverage to ensure that the different policies in place adequately cover the possible occurrence of the risk.

Where do you start?

The bottom line when looking at recovery planning is that as an organization you are putting practices in place in order to ensure your corporate livelihood. A different way to look at it is that the goal is to minimize downtown - that period where your organization is unable to provide the key product or service that makes your customers seek you out.

Starting the process can seem somewhat daunting, but the following eight steps provide a quick summary.

Step 1: Identify a planning and continuity coordinator. This is the individual who will be responsible for executing the plan and for driving the recovery efforts when/if the time comes. Splitting this responsibility across multiple functional areas or people is not a good idea.

Step 2: Identify each business unit's responsibilities and tasks. Identify recovery time requirements, prioritize those requirements, and determine the business unit dependencies.

Step 3: Identify subject matter experts who will help you create the recovery strategy and plan. Determine the business unit requirements for systems and services, offsite storage, and work group recovery environments.

Step 4: Collect appropriate documentation for IT operations. Determine critical applications and their priorities. List data required and document software dependencies/requirements.

Step 5: Identify all interdependencies between business units. Select team leaders, identify recovery locations, assign recovery locations by work group (some groups may have special needs). Consider costs. Estimate costs by function, business unit, and time.

Step 6: Identify application restoration requirements. Document the restoration procedures. Address any data synchronization requirements once data is recovered to a known state.

Step 7: Calculate hardware restoration time. Identify outside storage procedures, data retrieval procedures, and total time for systems to be available. Create business phone lists, including key vendor contacts, maintenance providers, specialized technicians/consultants as appropriate, and customer numbers.

Step 8: Finalize/review the document. Identify procedures for document control. Schedule recovery exercises and actually hold them. Ensure there is an ongoing evaluation process as your organization changes and matures.

Plan for Team Exercises

There are multiple approaches to exercising you completed plans:

Checklist Exercise

This determines whether adequate supplies are stored and/or identified for a fully functional recovery site. These supplies can range from PCs, printers, phones, notepads, pens/pencils, and so on. The goal is to ensure that the items and item quantities stays accurate.

Table Top Exercise

This type of exercise is used to simulate acquisition of information in a disaster situation:

- A recovery team is assembled around a table.
- A structured scenario is established.
- At time intervals, messages are fed to team members who generate specific responses.
- Team members describe their responses.
- Frequency of messages and urgency required is increased to simulate increased tensions.

Structured Conference Room Walk-through Disaster Simulation Exercise

For this exercise, business continuity team members meet to verbally walk through the specific steps of each component of the continuity process as documented in the plan. The purpose is to confirm the effectiveness of the plan and to identify gaps, bottlenecks, or other weaknesses in the plan.

Simulation Exercise

In this exercise, the organization simulates a disaster during non-business hours, such that normal operations are not impacted. Performing a review of the exercise can include notification procedures, temporary operating procedures, and backup/recovery operations.

Parallel Exercise

A parallel review exercise can be performed in conjunction with the checklist review or simulation exercise. Under this type of exercise, historical transactions, such as the previous day's transactions, are processed using the preceding day's backup files at the contingency processing or recovery site. Rep+-orts are generated and then validated against the same reports generated against production data.

Full-interruption Exercise

This type of exercise activates the total business continuity plan. These exercises tend to be costly and could disrupt normal operations and therefore should be approached with caution and adequate planning,

Regardless of the type of exercise, holding them is the key step. All are effective in their own way and provide the means for keeping the plan current.

During a Table-top review, a portion of the data backup plan was read aloud:

"Mary S. will take a snapshot of the shared network drive N:, write the contents to a CD, and store it in her basement, labelled with the date and time of the backup"

Putting aside the appropriateness of storing corporate back-ups at an employee's home, the reviewer was met with quizzical looks from the recovery team. Upon further discussion, it finally came out that Mary had left the organization 6 months earlier. Since that time, no back-ups had been created for that network drive, nor had any of the previous copies been retrieved from Mary's basement and secured for corporate use.

More timely reviews would have caught this sooner, and eliminated the huge risk that was unknowingly being assumed. Reviews should be held at least quarterly in order to ensure the accuracy and completeness of the plan.

Going Forward

This paper provides a broad brush overview of business continuity and disaster recovery planning. A key source for the contents in this write-up is the book authored by the founder of Huber Advisors, Robert C. Huber, RESPONSE! *Planning & Training for Emergency Recovery*

As Winston Churchill said:

"Let our advance worrying become advanced thinking and planning."

In terms of BCP and DR planning, rather than worrying about it, plan to recover from it.

If you'd like more information on the Huber Advisors approach to recovery planning, contact us at:
information@huberadvisors.com
651-429-9991

Also, copies of the RESPONSE! book are available for sale on the Huber Advisors website
www.huberadvisors.com