

Lessons from the frontline

Dr. Barbara Hillenbrand had her business continuity skills put to the test in the most extreme way; the plans she worked on were invoked during the 9/11 attack on the World Trade Center. In this article Barbara shares her thinking on how to develop a good business continuity plan.

As an IT auditor I have a unique perspective on disaster preparedness. I reviewed the disaster recovery plans of a foreign bank with operations based at the World Trade Center, not once, but twice before the 9/11 attack. The recommendations I made were implemented, tested and incorporated into the disaster recovery plan prior to 9/11. Due to the superb efforts of the emergency management team (EMT) our mission critical systems were fully restored to the hot-site after the attack. Moreover, the swift evacuation of employees from WTC towers one and two undoubtedly spared many lives.

The following article highlights the key planning phases and critical tasks that should be completed to ensure that your firm is adequately prepared when disaster strikes.

At the outset I suggest that you implement at least three of the following recommendations:

- * Hire one or more outside consultants to bring in the expertise your team is lacking. Consultants may be especially helpful during the business impact analysis (BIA) and testing phases of the project.
- * Customize templates and planning tools available on the Internet to suit the needs of your organization or business.
- * Contact the Office of Emergency Management to determine whether they provide disaster preparedness training to local businesses / organizations. Better yet, find out what type of training you will need and then ask their assistance in providing it.
- * Contact your local Chamber of Commerce; and fire, police and emergency medical services departments to determine ways to ensure better coordination between your business and local agencies and to reduce the number of civilian casualties at the disaster scene.
- * Attend business continuity and disaster recovery planning conferences and/or IT conferences (which include sessions on disaster recovery planning) to determine what other businesses within your industry are doing. Take advantage of networking opportunities. Experts will often divulge more and better information 'face-to-face' than via e-mail or any other form of communication.

The five things you should know before diving in:

1. Is there a business continuity plan (BCP) and/or emergency management team already in place? If so, then what will your role be?

2. What departments and/or functions will be involved? Talk with your project sponsor (e.g., the person who gave you this assignment) to see what type of arrangement makes sense, a plan based on cross-functional teams or one based on department-level teams.

3. Is there a project plan and overall project budget? If not, volunteer to put these together, but do so only after you have a clear idea of what will be needed. Do the business impact analysis first (see explanation below) and then return to this step.

4. Has there been discussion concerning likely disaster scenarios? If disaster scenarios were discussed at a recent board of directors meeting, then obtain a copy of the meeting minutes.

The seven phases of business continuity and disaster recovery planning are:

1. Business impact analysis (BIA) and risk assessment;
2. Project initiation phase;
3. Design and development phase;
4. Implementation phase;
5. Testing phase;
6. Maintenance phase; and
7. Execution phase.

The entire planning cycle takes three months to one year depending upon the size of the firm and complexity of the organization.

Some readers may wonder why I have placed the BIA/risk assessment phase before the project initiation phase. Actually these two phases can be performed in either order or can occur concurrently. I believe that before you begin planning it is best to have a clear idea of all potential disaster impacts and their cost to the business. Having this information at the outset allows you to prioritize and then focus your planning efforts on the most likely disaster/highest impact scenarios. The idea here is that resources are scarce and that indeed it may not be possible to mitigate all sources of risk to the organization at the outset, due to the prohibitive costs involved. The organization may have to consider 'tradeoffs,' implementing some controls now and other controls when additional funding becomes available. Planning efforts could be focused on mitigating those risks which are most likely to occur in the near future (e.g., floods, tornados, blizzards, fires) and implementing controls to address such disasters as a complete loss of access to the operating facility later on as resources are made available by the CFO and board of directors.

Now, let's begin planning!

Phase one – business impact analysis (BIA) and risk assessment

Most business organizations rely on technology and automated systems to such an extent that even a short-term disruption of 24 hours or less could result in serious financial loss. BIA is the process used: to identify potential threats to a business; to identify critical systems and functions that must be restored to resume normal operations following a disaster event; to identify the controls needed to reduce an organization's financial exposure; and to determine the cost of implementing such controls.

The 'critical objectives' to be achieved during this phase:

1. Identify all mission critical business processes; infrastructure and information systems.
2. Identify dependencies and interdependencies between the critical business processes/systems.
3. Identify organizational risks and potential threat scenarios.
4. Discuss likely recovery alternatives.
5. Determine the maximum allowable downtime for each business process. Determine the order in which business processes/systems should be restored.
6. Prioritize critical business processes by evaluating their potential quantitative (financial) impact and qualitative (non-financial) impact following a disaster.
7. Identify the type and quantity of resources required for the recovery (e.g., laptops, chairs, faxes/phones, desktops, printers, telephone handsets, and so on).
8. Determine what facilities will be available at the recovery site.

Recommendations:

* Have all mission critical departments, processes, infrastructure and information systems been identified? Probably not. The planning process is somewhat iterative - items will continually turn up that were previously overlooked. It pays to acknowledge this from the start and to develop a version control process to ensure that all changes in your planning documents are reflected as you go.

* If you are absolutely clueless at any point as to how to proceed, then look both inside/outside your organization for a consultant to guide you through this process. Find someone: easy to work with; who is trustworthy; who has mentoring/people skills; and who has business continuity and disaster recovery planning experience. Preferably find someone who will facilitate the BIA and serve as your advisor behind the scenes. Interview a number of people to find the right person. Do not overlook the human resources department or your IT trainer as internal sources of talent.

Phase two - project initiation

The steering committee, aka the emergency management team, is established during this phase. They will provide the leadership and direction for this project. A project sponsor is named if one is not already designated. In addition, department level disaster recovery teams (which will report into the steering committee) will be established at this time.

Critical objectives to be achieved during this phase:

1. Appoint a project sponsor and establish a planning/steering committee.
2. Develop a mission statement.
3. Prepare an overall project plan and budget.
4. Setup a reporting process to monitor the status of critical project tasks.

Recommendation: Meet once a week with members of your steering committee to jumpstart the planning process; once a rhythm is established and department-based recovery teams are immersed in planning activities you may wish to meet less frequently (e.g., biweekly, or monthly) to review the progress of individual team efforts.

Phase three - design and development phase (designing the plan)

The EMT develops a high-level recovery strategy in response to each threat scenario identified during the BIA.

Critical objectives to be achieved during this phase:

* The disaster recovery team will determine an appropriate department/function level response for each risk scenario.

Recommendations:

* Circulate a copy of the minutes for the BIA to your recovery team leaders. They can use this information to help identify appropriate department based recovery strategies for each risk scenario.

* You might request that the BIA facilitator return and meet with department/function heads to explain the BIA and to orient their thinking towards the development of department/function based recovery strategies. Have the secretary take the meeting minutes and circulate the minutes to everyone in attendance.

Phase four - implementation phase

The implementation phase is the most labor intensive of the seven business continuity planning stages. You will spend most of your planning hours here.

During this phase individual departments/functions will develop recovery plans in detail. Each department head should recruit staff within their area to assist in the planning and writing process. Web-based templates can be customized to facilitate the development of the recovery plans within the department and function-based units. Draft recovery plans should be reviewed and discussed by members of the department to ensure they are accurate and complete (prior to submitting them to the steering committee for further review). The steering committee should review the plans to determine what dependencies and inter-dependencies exist between them.

As you near completion of Phase 4, meetings of the EMT (or steering committee) will be used as a forum to: report on the progress of departmental planning efforts; discuss emerging threats in the business environment (e.g., in the news /journal articles); plan future tests of the disaster recovery plan; and to provide the EMT with updates of data and information (e.g., such as personnel changes).

Critical objectives to be achieved during this phase:

1. Define the recovery tasks (including sequence and timing) for each recovery team and assign roles and responsibilities.
2. Differentiate between the operational, technical and departmental recovery teams.
3. Identify dependencies/inter-dependencies and accountable individuals for each task.
4. Define escalation procedures.
5. Identify and list key contacts, vendor/suppliers and resources.
6. Structure and document the plan in such a way as to promote ease of use and future maintenance.
7. Select the most appropriate tools for creation and maintenance of the plan.

Documents which will be needed by the recovery teams:

1. Business continuity / disaster recovery plan, or template (if available)
2. Project budget and project plans (created during Phase 1)
3. Organization chart showing names and positions
4. Operations and administrative procedures
5. Relevant industry regulations and guidelines.

Recommendations:

* Use the implementation phase as a training opportunity for personnel at the department/function level. Host a day long project rollout. Consider inviting the human resources or information technology department to explain the planning template; the fire department to discuss fire safety procedures and the importance of monthly evacuation drills and a terrorism expert to discuss appropriate responses to bomb threats, kidnappings and other violent events.

* Use project management software (e.g., MS Project) to monitor the status and accountability for individual recovery tasks in your project plan.

Phase five - testing phase

During the testing phase the EMT (or steering committee) works with management to design appropriate testing procedures. A good test is one which provides a realistic view of what could go wrong during a disaster event. Desktop testing is often used because it is less costly and less risky than a test which processes a limited percentage of production data in a test environment.

Critical objectives to be achieved during this phase:

1. Define the testing strategies.
2. Select the testing method.
3. Define test objectives and prepare test plans.
4. Conduct testing.
5. Document testing deviations from expected results.
6. Prepare post-test report and meet with senior management to discuss the results.
7. Amend the business continuity plan based on post-test results.

Recommendation: As you would normally do, invite the audit department to observe the disaster recovery test in progress.

Phase six - maintenance phase

A process should be developed to ensure that the results of the tests are incorporated into the current version of the recovery plan document.

You have now complete one planning cycle. Unless there is a disaster you will never find yourself in Phase seven. Next year resume the planning process at Phase one. Until then, meetings of the steering committee should continue on a monthly basis.

Critical objectives to be achieved during this phase:

1. Determine ownership and responsibility for maintenance of the various BCP documents.
2. Identify the BCP maintenance triggers to ensure that all organizational, operational and/or structural changes are communicated to personnel accountable for maintaining the plan.
3. Determine the maintenance procedures required to update the plan.
4. Determine the procedures to ensure that the plan is kept current.
5. Implement version control procedures over the plan document.
6. Continue monthly meetings with the steering committee, test the plan on a biannual or annual basis and repeat the BIA annually.

Phase seven - execution phase (declare disaster and execute recovery options)

During a disaster, the recovery plan should be used by the departments and/or the functional areas to restore business operations. Daily status reports of recovery activities should be issued to senior management to ensure that they are adequately informed of the progress of recovery operations. Working from a plan will provide focus in an otherwise chaotic emergency situation.

During the recovery from the WTC disaster, I attended team status meetings in the systems areas and took minutes concerning the progress of the recovery efforts. These minutes were used by managers in my area to prepare the daily status reports that went to our headquarters in Tokyo, Japan.

Critical objectives to be achieved during this phase:

1. A member of management (with the proper authority) declares a disaster.
2. The recovery teams implement the disaster recovery plan.
3. Monitor expenses incurred during the disaster/recovery effort.
4. Provide daily status reports to senior management.

Documents/deliverables which will be needed at various planning phases:

1. Staff emergency contact information
2. List of vendors/suppliers and their contact numbers
3. List of emergency services and contact numbers
4. The premises addresses and maps
5. Health, safety and evacuation procedures
6. List of consultants/professional advisers and their emergency contact information
7. Personnel administrative procedures
8. Business unit policies and procedures
9. Copies of floor plans
10. Asset inventories
11. IT inventories
12. IT system specifications
13. Communication system specification
14. Copies of maintenance agreements/service level agreements
15. Off-site storage (backup) procedures.

About the author: Dr. Barbara Hillenbrand hails from the Midwestern region of the US. She moved to New York City to pursue first a MA at Hunter College and then a MS in IT and Performance Audit at New York University's Robert F. Wagner School of Public Service. As her career and academic interests converged she applied and was accepted into the Doctoral of Professional Studies program at Pace University's Lubin School of Business. She received her Doctorate in Economics in 2005 and has recently been consulting in the area of business continuity and disaster recovery planning.

BrbrHillenbrand@aol.com