Subject Matter Areas Information

Areas of Disaster Recovery / Business Recovery Management include:

1. Project Initiation and Management

What did you do with regards to *Project Initiation and Management*?

For multiple consulting clients and companies that I have worked for, I was responsible for identifying why management should fund recovery operations along with the need to fund the creation and maintenance of recovery plans. Some of the reasons I provided to management in support of recovery operations included:

1. Establish a Steering Committee and management structure to support recovery planning. This committee and organizational structure would be responsible for making all management decisions regarding recovery planning and was the group I reported to.
2. Assist client sponsors in defining recovery objectives, policies, and critical success factors. This funding should include initial BCM creation and the maintenance of BCM functions going forward.
3. Identify compliance needs that must be met and review existing controls that are designed to respond to compliance requirements. Rate compliance controls to insure that they are providing accurate responses to compliance needs. If not, then determine what needs to be accomplished to mitigate the exposure and any additional costs associated with implementing the changes. Report findings to management.
4. Formulate scope and goals related to recovery planning and gain management approval for strategic, tactical, and operational plans.
5. Created a project plan that identifies the steps that needed to be taken to develop recovery plans, testing procedures, and maintenance procedures for recovery plans. Identified skills needed to

perform tasks so that management can assign personnel with the required skill set needed to complete project tasks. Integrate recovery procedures within the everyday function performed by the staff to insure that recovery plans are always current.

6. Present project plan to management and gain approval for the project. Make any changes recommended by management and finalize plan.
7. Management issues a memo / email to personnel outlining the BCM process and directing them to cooperate with the development and maintenance of recovery plans.
8. I then assumed management of the recovery project plan and periodically reported to the Steering committee and Recovery Organization.
9. An immediate goal of any plan was to safeguard personnel by providing them with a means to escape a disaster event. Practice exercises were used to ensue that personnel know where to go in a disaster and how to get their as quickly as possible in order to minimize confusion. Similar to "General Quarters" drills exercised by the military to improve the ability to counter an attack, these drills would reduce the amount of time needed to evacuate when a disaster event occurred and thereby reduce casualties.
10. Perform a risk analysis to identify and classify risks and the controls in place to lessen the risk (i.e., sprinkler system and fire suppressant systems, etc.). Also to ensure that existing controls are sufficient to overcome the risk (i.e., water sprinklers in a paper storage area are not good controls and the costs associated with updating the fire suppression system to replace water with chemical fire suppressants should be calculated during the Risk Assessment and provided to management in the final report).

How did you do it?

In most cases management already knew that they needed to develop recovery plans, but were not committed to supporting the project and its associated costs. Also management did not know how many people would be required to staff recovery positions and assist in the: development, testing, support, and maintenance of recover plans. This information was provided in the management report that was created as a result of the Risk Assessment. In order to convince management of the need to commit to the development and maintenance of recovery plans it was necessary to identify exposures and responsibilities associated with management's need to develop and support recovery planning. The goal of this initiative was to make management aware of their need to fund the recovery process through management commitment and monetary support.

This was accomplished by identify management responsibilities for protecting their business from prolonged outages that could interfere with the continued supply of services or products and the impact this disruption would have on the company's bottom line and reputation. Any compliance issues and requirements were also discussed to define the need for BCM and the safeguarding of critical compliance information.

Once management was convinced that they should support recovery planning, the Scope and Objectives associated with recovery planning were formulated and a project plan developed to meet recovery planning needs. This plan was presented to management for their acceptance.

A steering committee was formulated to oversee recovery planning and a member of Senior Management was selected as the recovery coordinator. This person is the main contact that the recovery planner communicates with.

At this point management is approached to provide a budget for recovery planning and maintenance. This budget will illustrate management's commitment to the recovery and compliance process.

The final result of the project initiation exercise is to start a recovery planning program (Funding, Resources, Multi-Year Maintenance) including: Development of Recovery Plan Objectives (Action Items, Relative Importance, Sequence of Events), Development of a Recovery Planning Project Plan (Specific Recovery Plans for a range of Disaster Events, including sequence of events and time requirements), and finally the creation of a Recovery Process to support recovery planning in an on-going basis.

How long did you do it?

I have over 25 years of experience for multiple employers and consulting clients performing this service for: MHT, Chemical Bank, Chase Bank, SIAC, NY Stock Exchange, RMJ Securities, European American Bank, Bank of America, Merrill Lynch, Soloman Brothers, The United Nations, and Sandoz Pharmaceuticals.

2. Risk Evaluation and Control

What did you do with regards to *Risk Evaluation and Control*?

In this stage of the Recovery Project, I was responsible for identifying and rating risk exposures and any controls that may be in place to mitigate a risk (probability – consequences/impact). I then had to identify controls that were for general use and did not provide risk mitigation, like water sprinklers in a paper storage room.

I had to identify internal and external personnel needed to support recovery planning by defining the skills and time requirements associated with recovery planning.

Working with the recovery teams, it was determined which controls needed to be implemented to mitigate risks. The costs associated with these controls and the amount of time needed to implement the controls were also calculated. I then provided management with a report on the identified risks to determine the acceptable risk level of the organization. From this meeting, risks were rated and the basis for a recovery operation formulated.

The final report to management identified the financial impact of disaster events and gained management support for building and maintaining the recovery plans.

The tasks performed during the risk evaluation included conducting physical inspections of offices and IT locations to determine what risks were in the location and what actions were needed to mitigate the risk. These inspections included fire suppression, breathing devices, fire extinguishers, locked doors and fire stops. Both internal and external exposures were identified and documented during this process.

Once the physical inspections were completed, logical inspections were conducted to determine if IT backups were taken on a regular basis and that backups were stored in safe locations. I also determined if compliance and regulatory requirements were being adhered to and what actions were being taken to comply. Also the auditing department was asked to contribute by identifying any additional requirements that had to be adhered.

How did you do it?

When performing a risk analysis, I usually started with a floor layout and organizational structure. I then identified any compliance issues associated with the company and its industry. After management issued a supportive memo instructing company personnel to cooperate in the recovery planning process, I established a schedule for performing a physical inspection of locations to identify risks and controls that were in place. Information gathering techniques were also developed and forwarded to the departments and locations to be inspected. These forms helped information gathering and reduced the amount of time needed to evaluate risk exposures. Any risk that did not have a corresponding control was also identified. The costs associated with implementing a control to mitigate specific risks was obtained and added to the management report along with the impact of not implementing the recommended controls.

Reporting on the qualitative and quantitative results of the risk evaluation to management made them aware of the costs of existing risks, the amount of money needed to implement suggested controls, and the impact of a disaster event on the continuation of business and the loss of reputation that would be associated with a disaster event (consider Jet Blue and Taco Bell events and the impact they had on company reputation and business).

IT Security and Vital Records Management concerns were identified during this phase, because compliance and recovery requirements need to identify critical data and the procedures used to safeguard this information against unlawful access and loss. Any automated storage management systems in use, along with IT security and vaulting procedures, were evaluated to confirm their ability to protect data and adhere to compliance requirements.

Industry Best Practices described in COSO and CERT documents were used as a guideline during this process to insure all critical issues were addressed.

Management would then determine their tolerance to risk and which risks should be addressed. This led to the development of the projects scope and objectives.

Major areas of concern were identified as a result of the Risk Evaluation, such as: Data Sensitivity (who owns data, its importance, access controls, and backup / recovery requirements), Vital Records Management (backup, vaulting, and recovery of critical data files), and Change Management procedures to ensure that recovery plans are maintained in a current manner.

How long did you do it?

Over 25 years of experience for employers and consulting clients including: MHT, Chemical Bank, Chase, Citibank, European American Bank, AIG, ADP, RMJ Securities, Computer Science Corporation, and IBM.

3. Business Impact Analysis

What did you do with regards to *Business Impact Analysis*?

Performing this function for multiple consulting clients and at positions I held at the companies I worked for, I performed the following work with regards to performing a BIA:

1. Determined which locations needed to have a BIA performed.

2. Identified location personnel who would participate in the BIA and be responsible for BIA activities for the location going forward.
3. Created BIA forms that would be used to identify critical functions and personnel, infrastructure requirements (floor space, electricity, HVAC, etc.), technology requirements (server, applications, data files, specific equipment, interfaces, etc.), facilities (desks, phones, fax machines, etc.), and special forms needed to support location.

4. Identified Vendors and Suppliers to determine their ability to continue to supply locations if a disaster event occurred at the business or supplier location and insure Supply Chain functionality.
5. Entered information from multiple locations into BIA forms.
6. Combined information from forms to identify most critical locations and the resources needed to support them.
7. Gained management approval of analysis and permission to move forward.
8. Identified common recovery practices that could be used across locations.
9. Defined Recovery Time Objectives and Recovery Point Objectives from information and conversations with Location Representatives and Information Technology Department.
10. Formulated final report to management and gained approval to go forward with the recovery process.

How did you do it?

After first defining the organizational structure of the client company and identifying the locations where a BIA is to be performed, I had management forward a memo (email) to location managers telling them that I would be working with them to create a BIA. I then developed BIA forms and met with location management to discuss the information that must be entered into the forms and how best to obtain the information. I then worked with location personnel to ensure that BIA information was correctly obtained and entered into the forms. Combining the information contained in all of the forms made it possible to identify and rate critical business operations and common recovery practices.

Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) were used to determine the types of data recovery and vital records management that were needed to support Business Recovery. Working with the IT department and management made it possible to identify the best practice needed to support data recovery needs and Recovery Time Capability (RTC) currently in existence. After putting all of this information together, I generated a final report to management and tried to gain their support for development of recovery plans going forward.

In some cases, clients had already purchased recovery planning tools like LDRPS. When this occurred, it was necessary to train location personnel on the recovery planning product. In other cases we developed our own BIA forms and used them to perform the BIA.

The objective of a BIA is to identify and rate locations as to their recovery requirements, the staffing needed to develop recovery plans, and the amount of time associated with their being able to recover operations. By examining RTO, RPO, and RTC findings, it is possible to determine what has to be accomplished to meet management guidelines associated with recovery priorities.

How long did you do it?

Over 25 years of experience for employers and consulting clients including: MHT, Chemical Bank, Chase, Citibank, European American Bank, AIG, ADP, RMJ Securities, Computer Science Corporation, and IBM.

4. Developing Business Continuity Management Strategies

What did you do with regards to *Developing Business Continuity Management Strategies*?

Based on the Recovery Time Objectives, Recovery Point Objectives, and Recovery Time Capability a strategy was developed to insure that data and IT processing requirements were available along with business office facilities. This requirement was used to ensure that vital records were backed up and stored in off-site vaults, where they would be recoverable within the Recovery Time and Recovery Point Objectives developed during the BIA process. Sometimes the RTO and RPO requirements were too short for recovery using vaulted resources, so storage management systems were used to support Recovery Time Objectives. Recovery facilities, offered by vendors or included within the client's environment (remote computing facilities and business offices that were capable of internally supplying recovery services and facilities) were identified and the costs of using these services determined. The advantages and availability of supportive services were then categorized and their costs documented. IT and business management were then consulted to determine their ability to provide recovery services and to gain consensus on the best strategy to follow. Finally, a report to management was created and presented to gain approval to continue building recovery plans.

In many cases, the best recovery strategy is to do it internally by separating IT facilities into multiple locations, each capable of backing the other site up. Should site 'A' suffer a disaster, its processing could be supported by site 'B' or site 'C'. In other cases, it is essential to develop an enterprise policy that would make it a requirement to purchase compatible machinery so that recovery operations can be developed internally. For example, if a manufacturing company had three locations and each location created fabric for the fashion industry, it would stand to reason that each site contain similar equipment that would be capable of picking up operations for a failing site and keeping customer orders filled.

How did you do it?

I helped develop recovery strategies by working with management when I was an employee, as an Agent for IBM Recovery Services, when represented Zurich Depository (Vaulting service), and as an Engagement Manager in the Technology Risk Management area of Jefferson Wells. I also developed recovery strategies for a range of consulting clients and employers. In these roles, I was responsible for identifying various recovery strategies (both internal and external to the organization) and for presenting these findings through management reports and presentations.

The goal of the presentation was to make management aware of their recovery needs, the available strategies that they could take advantage of, the costs associated with these strategies, and the time needed to implement recovery strategies.

Every company may need a different recovery strategy. Today many large firms ensure their ability to recover quickly, or instantly, by utilizing an internal recovery strategy. This strategy requires multiple data centers and a data management system that can keep data in sync with the primary and recovery site on a mirroring or incremental basis. This process is cheaper and more efficient than going to an outside vendor location like Comdisco and can be easily integrated within an organization. Some sites are used for Development, Maintenance, Testing, and Quality Assurance, while the other data centers can be used to support Production Operations. Should the production site fail, it would be possible to fall back to the maintenance data center - especially if enterprise controls are in place.

How long did you do it?

Over 25 years of experience for employers and consulting clients including: MHT, Chemical Bank, Chase, Citibank, European American Bank, AIG, ADP, RMJ Securities, Computer Science Corporation, and IBM.

5. Emergency Response and Operations

What did you do with regards to *Emergency Response and Operations*?

I have been responsible for identifying the potential types of emergencies that would be experienced (fire, flood, tornado, snow, electrical failure, or any emergency that would stop people from being able to travel to or function at work) and the responses needed to mitigate these exposures. I examined existing documentation to determine if any response plans are in place and if the plans are sufficient. I then proposed the development of Emergency Procedures where none existed or where existing plans were not sufficient.

It was then my responsibility to integrate Emergency Response plans with Disaster and Business Recovery Planning. For example, should we experience a fire, all personnel would be evacuated and the fire and police departments would take control of the scene. If it was determined that the scene would not be returned beyond acceptable Recovery Time Objectives, Disaster Recovery Plans would be immediately initiated.

Once the emergency responders left the scene and turned it over to the company, recovery plans associated with evaluation, salvage, restoration, and recovery would be initiated to either activate/remain at remote facilities or restore operations at the original site. This decision was usually made based on RTO and RPO requirements.

A Contingency Command Center was created and staffed when the emergency was first identified. Management staffed the Contingency Command Center and was responsible for making any decisions needed to restore operations, communicate with the outside world and staff, and to generally monitor and respond to disaster events as they occurred. Coordination with emergency responders and recovery facilities were coordinated through the Contingency Command Center and the Emergency Operations Center manned by first responders.

How did you do it?

When developing recovery plans it is essential to understand emergency responder activities and their control of the disaster location. This is because you will not be able to get into your site until the Emergency Responder or External Agency completes its work and allows you to return to the facility.

To better understand how emergency responders treat a disaster scene and the best method for communicating with them during the disaster event, I often sought out emergency responders to discuss these subjects prior to a disaster event. I am also a member of the Contingency Planning Exchange (CPE) and the Association of Contingency Planners (ACP), where emergency responders are often speakers. These meetings provided speakers from firms that actually experienced a disaster event so that we could all benefit from the lessons learned by presenting companies.

After learning as much about emergency responders as I could, I was better able to integrate recovery plans and emergency response procedures with recovery plans. This allowed companies to know when to activate recovery teams and the sequence that best suited the disaster event. Working with the emergency responders and knowing how long they expected to be in control of the disaster site also allowed us to better understand when we should declare a disaster and move operations to recovery facilities.

Lessons learned by emergency responders allow companies to better identify external risks and establish controls that could mitigate the risk. These risks included single-point-of-failures associated with external agencies like the phone company. In most cases, phone companies have only one exchange servicing a location. They also provide telephone services through a telephone cabinet located in the basement and risers that move telephone calls to corresponding floors for routing to the desktop. With this knowledge it is possible to identify alternate suppliers that could supply services from a different exchange and routing operation, thereby eliminating a single -point-of-failure usually without any additional costs. Many lessons learned from external agencies and first responders can result in a safer environment and fewer disaster events.

How long did you do it?

Over 25 years of experience for employers and consulting clients including: MHT, Chemical Bank, Chase, Citibank, European American Bank, AIG, ADP, RMJ Securities, Computer Science Corporation, and IBM.

6. Developing and Implementing Business Continuity and Crisis Management Plans

What did you do with regards to *Developing and Implementing Business Continuity and Crisis Management Plans*?

When I was responsible for creating Business Continuity and Crisis Management Plans it was important to define the range of recovery plans that needed to be developed, the people who would be responsible for recovery tasks, where the people must meet in the event of a disaster, and the tasks that they are responsible for performing in the sequence that these tasks must be performed. The recovery plan had to be able to mitigate the risks identified earlier and for the elimination of any single points of failures that had been identified. Sometimes tools were used to develop recovery plans (i.e., LDRPS) and recovery personnel trained on these tools.

The goal of a recovery plan is to reduce the consequences of a disaster event to a service level deemed necessary by management, so it is important to first respond to high impact disasters and then develop plans for those disasters that are deemed less of an impact by management. Recovery plans must include: who is on a recovery team, what tasks that person should perform when responding to a disaster, where resumption operations will be performed, when business operations must be resumed, and any procedures needed to recover, resume, continue and restore operations. Recovery plans must also be categorized as Business Recovery (Offices), Disaster Recovery (IT), and Emergency Response Plans (Public Services like fire, police, etc.).

Recovery plans must be clear concise and written in the sequence that they must be performed. Coordination with suppliers, vendors, and management must be on-going and often, so that proper decisions can be made and required resources made available to recovery teams.

A crisis communication plan must be included in recovery planning, so that the right company representative can keep personnel and the media informed of the disaster event and recovery activities. It is important to have separate communications plans for radio, TV, printed press, and the internet. Having these communication statements developed in advance will allow a company to better represent itself and lessen the impact of a disaster event on the company's reputation because of statements made to the media and stakeholders.

How did you do it?

I have been responsible for creating recovery plans for banks, brokerage firms, manufacturing firms, pharmaceutical firms, and a range of other business organizations. These plans would be separated into Emergency Response Plans, Business Recovery Plans, and Disaster Recovery Plans depending upon the location and range of a disaster event. I have also utilized various automated and manual tools to assist in the development of a recovery plan (i.e., LDRPS, DRS by Tamp, etc.) as well as developing forms and plan outlines in-house.

When developing recovery plans, I first identified the range of disasters that had to be responded to. I then located team members and met with them to define roles and responsibilities. We then formulated a recovery approach and documented the approach within recovery plans in clearly written sequential instructions. Vendors and suppliers were identified and included in appendices for quick reference. Suppliers were used to route needed supplies to the recovery facility, while vendors were used for Vital Records Management and Recovery Facilities.

Plans were developed and tested using table top and real life recovery scenarios. Plan testing included: Unit, System, and Regression tests. Plan maintenance requirements were documented and plan distribution procedures created. Discussions were also conducted to determine how to best integrate recovery procedures within the everyday functions performed by personnel, including the Systems Development Life Cycle (SDLC), Program Development Life Cycle (PDLC), Support / Incident Management, and Change / Maintenance / Version and Release Management procedures.

As a result of these planning efforts, my clients and employers were better prepared to recovery from a range of recovery events in an on-going manner.

How long did you do it?

Over 25 years of experience for employers and consulting clients including: MHT, Chemical Bank, Chase, Citibank, European American Bank, AIG, ADP, RMJ Securities, Computer Science Corporation, and IBM.

7. Awareness and Training Programs

What did you do with regards to *Awareness and Training Programs*?

As part of a disaster recovery planning effort, it is important to make employees, vendors, suppliers, and first responders aware of the recovery objective and effort used by organization. Coordination procedures between the company, clients, external agencies, and first responders can also be developed to better respond to disaster events. Once defined, this information can also be included in awareness and training programs.

Developing awareness and training programs will provide employees and recovery team members with a better understanding of recovery goals and procedures. Initially, posters can be developed and placed at strategic locations throughout the company. These posters should provide personnel with a clear overview of the recovery process and its goals.

Once recovery teams have been formulated, providing them with specific training related to creating and maintaining recovery plans is essential. Personnel should be made aware of their tasks and trained on how to achieve their assigned responsibilities. If recovery personnel are using tools to support the recovery effort (i.e. LDRPS), then they should be trained on those tools as well. Cross-Training and Awareness of team member functions and responsibilities will help recovery personnel and management know who to contact for specific recovery information and direction sand should be included in training and awareness sessions.

Finally, lessons learned exercises should be conducted after recovery tests or real world recovery events. This information would be discussed and any changes to recovery plans and training performed. Industry disaster events affecting other firms or communities should also be examined to incorporate lessons learned by others and reduce the likelihood that the event would impact your firm as badly as it did firms that were not prepared.

Having a well trained employee is the first step to a successful recovery program, but insuring that personnel are included in recovery tests is the most essential aspect of training and awareness programs. Schedules for training exercises should be developed so that the widest audience possible gets an opportunity to review their recovery tasks. This will insure a speedy and safe recovery process.

How did you do it?

I have developed recovery posters, classes, and exercises to assist recovery personnel better understand their roles and responsibilities. When recovery tests or actual events are experienced, I have monitored the progress and noted any weaknesses that occur. Afterwards a review of recovery events is performed and weaknesses discussed. Corrective actions are agreed upon and added to recovery plans and training.

Awareness programs include posters and intranet write-ups that describe recovery planning and the tasks performed by various recovery teams. Making recovery training available to personnel in different forms will allow individuals to choose the form of training that best suits them. Providing a check-for-understanding after recovery training will test personnel's understanding of recovery procedures and route them back through training sessions related to any wrong answers. This process will ensure that personnel truly understand the recovery process and their involvement.

I have created presentations for the CPE, ACP, ISACA, and IFSA groups along with various companies and their recovery personnel. The purpose of these presentations is to make people aware of new developments and products that support the recovery process, while gaining feed-back from professional organizations.

The goal of an Awareness and Training program is to:

1. Establish training and awareness objectives and the components of awareness and training programs.
2. Identify functional awareness and training programs that are already in place.
3. Acquire or develop training and awareness tools.
4. Coordinate training and awareness with the HR department.
5. Identify external awareness and training opportunities and user groups.
6. Identify alternate options for training and awareness programs.
7. Define Certification Institutions like DRII and BCI to train and certify recovery personnel.
8. Incorporate various approaches to training and awareness so that personnel can choose the method they feel most comfortable using.
9. Provide personnel with certificate of completion after training is achieved.

How long did you do it?

Over 20 years experience for employers and consulting clients including: MHT, Chemical Bank, Chase, Citibank, European American Bank, AIG, ADP, RMJ Securities, Computer Science Corporation, and IBM.

8. Maintaining and Exercising Plans

What did you do with regards to *Maintaining and Exercising Plans*?

Once created, recovery plans must be periodically reviewed for accuracy and updates made as needed. To ensure that recovery plans are maintained in a current fashion, it is important to identify critical operations and applications and to modify the Change Management process to define the need to have updated recovery plans for changes made to critical operations and IT functions / facilities.

Besides normal changes made to operational areas (facilities, personnel, etc.) and IT Applications change requirements are identified during recovery tests or recovery events. After identifying the problem area, a decision is made as to the best way to eliminate the problem or enhance the recovery plan. In either event, a change is needed. Following change management procedures, a change request is completed and change management procedures followed to implement the enhancement or repair the problem.

After a change is made, testing has to be performed to make sure the change is implemented correctly. If the change is acceptable, then it must be communicated to team members, vendors, suppliers, and first responders as needed. Should training and awareness programs be updated, then they are and people made aware of the changes.

How did you do it?

I have been responsible for coordinating recovery plan changes and updates with the Change Management group for many companies. My responsibility would be to identify recovery plan changes, complete change requests, and follow the change process until the change is successfully tested and implemented. In some cases, I suggested that changes to recovery plans accompany any changes to applications or operational business areas. By hooking existing systems and procedures to include change management for recovery planning, it was possible to coordinate changes to operations with the changes needed to recovery plans.

I sold the Docu/Text and Job/Scan products, which were used to support change management and testing for applications. Incorporating recovery plans with the applications documentation made it possible to automate the turnover process for changes made to applications and their recovery plans. The recovery plan would be considered a separate document contained in a file and part of the job turnover requirement. If changes to applications included areas covered in recovery plans, then the recovery plan had to be updated to reflect the change. This process allowed for recovery plans to be treated like any other object that could be under the control of a movement product like Endevor in adherence with Version and Release Management guidelines. Whenever the application passed quality assurance, it would be moved from the testing environment to the production environment.

How long did you do it?

Over 25 years of experience for employers and consulting clients including: MHT, Chemical Bank, Chase, Citibank, European American Bank, AIG, ADP, RMJ Securities, Computer Science Corporation, and IBM.

9. Crisis Communications

What did you do with regards to *Crisis Communications*?

Crisis communications is responsible for providing media outlets (TV, Radio, Print, and Internet) with press releases that describe a disaster event and the actions being performed by the company in response to the event. Additionally, internal stake holders and external agencies must be communicated with during a crisis and these needs must be addressed during this process as well. If the company resides in a Commercial / Business Park then other companies co-hebetating in the area and other community residents should be notified of a disaster event so that they can take precautions as deemed necessary to continue their business operation and protect their staff of family. Any casualties or damage to the organization is provided along with the recovery operations being performed.

Crisis communications is performed by a designated company representative, who should be instructed to be honest and straight forward when discussing the disaster and the actions being performed by first responders and company personnel.

When implementing a crisis communications plan it is important to:

1. Have communications plans developed in advance of a disaster event, so that quick responses to media inquiries can be accomplished.

2. Identify a Crisis Communications Coordinator and make sure that person is aware of the crisis communications that have already been developed. It is also important for the crisis communicator to understand how the company wants him to respond to media inquiries.
3. Consider using Social Media to communicate a disaster event and instruct personnel, clients, and the community of the event and your actions.
4. Identify stake holders and make sure communications plans are in place to keep these stakeholders informed of recovery activities and the extent of the disaster on business operations.
5. Communications plans should be exercised along with the recovery plan and any weaknesses identified so that they can be updated through a change control.

How did you do it?

I have worked on crisis communications plans for a number of firms as a member or manager of the recovery planning process. I have also attended many presentations from media representatives on crisis communications. Although I have never been designated as the Crisis Coordinator, I have worked with many Crisis Coordinators to make sure they are aware of what is required of them and to implement changes and updates to media communication plans.

When creating a crisis communications document, it is important to tailor the document to a specific group (media, internal stake holders, external agencies, etc.). This is because TV uses visual representation to support audio statements and it is important not to have a burning building behind you when making a statement that you expect operations to be up and running shortly. When releasing crisis communications to print and radio stations, be sure to also place a statement on the company internet site. This will reduce the chance of being misquoted by news print and radio reporters. When asked for comment, you can simply direct inquiries to the web site and thereby ensure that the statement you want delivered to the public is yours and not distorted.

Crisis communications must also be developed for internal stakeholders, employees, and external agencies. Each of these documents should be tailored to the audience it is intended for. Employees need to know how they can support recovery operations by reporting to a specific area or performing work from home. Internal stakeholders need to understand the impact on the company's ability to deliver services and products, so that they can coordinate better with customers and take actions to help get operations back as soon as possible. External agencies must know who to contact for information related to company operations and facilities and how best to coordinate actions with the Contingency Command Center and Emergency Operations Center.

All of these communications documents must be identified and developed. Having them available will quickly establish crisis communications, reduce anxiety, and aid in the recovery of the business with the lowest loss to reputation and business operations.

How long did you do it?

Over 25 years of experience for employers and consulting clients including: MHT, Chemical Bank, Chase, Citibank, European American Bank, AIG, ADP, RMJ Securities, Computer Science Corporation, and IBM.

10. Coordination with External Agencies

What did you do with regards to *Coordination with External Agencies*?

Communications and coordination with external agencies is critical when developing Emergency Response Plans. In order to make sure your Emergency Response Plan is accurate and that people are informed of the amount of time before the site will be back, it is essential to learn how best to communicate with first responders. I visited firehouses, met with police officials, and attended many presentation on how first responders operate. After gaining a better insight about how external agencies operate, I established liaison procedures for each of the emergency responders and developed procedures for coordinating recovery efforts with the emergency responder. I also had to gain an understanding of the laws and regulations governing the company I was developing recovery plans for. The recovery plan had to be able to maintain regulatory requirements, even in a recovery environment.

Once all of my research was performed, I had to make sure that the company kept pace with any new development from the first responder or external agency. Recovery plans were updated as needed due to updates to external agencies (usually kept in the appendix of the recovery manual for quick reference).

Whenever possible, I asked external agencies and first responders to review our recovery plan to insure that we were coordinating our activities to the best of our abilities. In some cases I actually visited a recovery exercise being conducted by an external agency or first responder. In NYC this happens on a frequent basis and we have established an excellent rapport with external agencies and first responders through the Contingency Planning Exchange and Emergency Operations Center.

How did you do it?

I have worked with external agencies and first responders many times throughout my career and have realized their importance to recovery planning. Through presentations at the CPE and ACP meetings with people like Joe Bruno and Ira Tannenbaum (NYC EMO), I have gained a strong understanding of what external agencies and first responders do and how best to coordinate activities with them. During a presentation by Admiral Thad Allen, I was able to better learn how the government responds to disaster events like Katrina and the BP Oil Spill.

I have been responsible for developing many recovery plans for a large audience of companies (both as an employee and as a consultant) and in every case it was necessary to work with external agencies and first responders to make sure our recovery plan was as good as it could be. Working with these people and organizations has increased my knowledge of recovery planning.

The purpose of coordination with external agencies is to establish procedures for coordinating response, continuity, and restoration activities with external agencies and internal personnel, thereby expediting the recovery process. It is therefore important to identify external responders and establish a liaison with them. After a while it will be possible to create procedures for interacting with the external agency and to participate in recovery testing of each others recovery plans. The external agencies include compliance groups. By coordinating activities with these agencies, it will be possible to maintain current compliance knowledge relating to new laws and acceptable recovery procedures.

How long did you do it?

Over 25 years of experience for employers and consulting clients including: MHT, Chemical Bank, Chase, Citibank, European American Bank, AIG, ADP, RMJ Securities, Computer Science Corporation, and IBM.