

EMGT 835 FIELD PROJECT:
*Managing the Business Continuity
of Information Technology*

By

Jeremy Kissell

Master of Science

The University of Kansas

Fall Semester, 2008

**An EMGT Field Project report submitted to the Engineering Management Program
and the Faculty of the Graduate School of The University of Kansas in partial
fulfillment of the requirements for the degree of Master of Science.**

Herb Tuttle **Date**
Committee Chair

Tom Bowlin **Date**
Committee Member

Robert Zerwekh **Date**
Committee Member

Table of Contents

List of Figures	iii
List of Tables	iii
Acknowledgments	iv
Executive Summary	v
Abbreviations and Acronyms	viii
Chapter 1 Introduction	1
Chapter 2 Literature Review	3
Chapter 3 Increasing Motivation for the Planning Process	8
Chapter 4 Challenges to Information Technology Business Continuity	14
Chapter 5 Risk Assessment	20
5.1 Determining Mission Critical Components	
5.2 Analyzing Potential Threats	
5.3 Postulating Threat Impact	
Chapter 6 Designing a Plan for Crisis Mitigation	22
6.1 Establishing Plan Goals	
6.2 Identifying Critical Personnel	
6.3 Listing Mission Critical Hardware	
6.4 Recording Key Vendors and Suppliers	
6.5 Data Recovery Procedures	
Chapter 7 Testing and Acceptance	27
7.1 Practicing the Plan	
7.2 Continuing Education	
7.3 Gathering Feedback	
Chapter 8 Plan Maintenance	31
8.1 Identifying Plan Weaknesses	
8.2 Planning for a Better Plan	
8.3 Scheduled Plan Reviews	
8.4 Disaster Checklist	

Table of Contents (continued)

Chapter 9	Technologies Which Enhance Business Continuity	
	10.1 Voice Over IP	34
	10.2 Remote Access	
	10.3 Hosted Services	
	10.4 Clustered Servers	
	10.5 Wireless Networks	
	10.6 Redundant Array of Inexpensive Disks and Storage Area Network Usage	
	10.7 Off-site but Not Off-line Backups	
Chapter 10	Conclusion	40
	References	41

List of Figures

Figure 1: Business Continuity Planning Life Cycle.....8

Figure 2: Actual Causes for Data Loss..... 12

List of Tables

Table 1: Abbreviations and Acronyms..... v

Acknowledgments

This Field Project is dedicated to all the friends and family whose love for me is intensely felt. They have once again endured a period of absence and neglect which they did not choose. They did so knowing it will not be the last time a project, obsession, or opportunity will consume my focus and free time. I feel a great affection for those who have stuck by me and supported me during my work on this project and throughout the entire program. Everything that I am or do is a result of the luck of having their love.

I would also like to thank the faculty and staff of Engineering Management who have made my studies a positive life experience that was full of personal growth. Specifically, I would like to thank my committee members: Herb Tuttle, Tom Bowlin, and Robert Zerwekh.

Executive Summary

This field project is intended to provide a guide to overcoming the challenges to business continuity planning in IT. The need for business continuity planning is very real, yet this need is largely unfulfilled for many organizations. The goal of this project is to provide a concise and pragmatic collection of information necessary to guide an organization into preparing to respond to a disaster. Using the information provided here, an organization will be able to have a good grasp on what they need to do in order to be ready and able to recover from an event which results in the loss of part or all of their digital information.

The breakdown of this Field Project Document is as follows:

- Chapter 1 is an introduction to this research.
- Chapter 2 is a brief review of the literature used to gather information for this project.
- Chapter 3 investigates the reasons why many organizations do not have a BCP, and focuses on ways which can generate enthusiasm and support to make planning a priority.
- Chapter 4 is a discussion on the challenges commonly faced with the IT aspect of business continuity.
- Chapter 5 is a discussion of the risks an organization faces which may threaten the continuity of business.
- Chapter 6 covers how to develop a plan for response in the event of a catastrophe.

Managing the Business Continuity of IT

- Chapter 7 is a guide to the importance of testing and acceptance of a BCP.
- Chapter 8 covers the importance of plan maintenance and why vigilance in the planning process is vital to success in a post-disaster environment.
- Chapter 9 reviews several available technologies and how they may be leveraged towards creating an environment that can survive a disaster.
- Chapter 10 is a summary and conclusion of the project.

Acronyms (or Abbreviations)

Acronym	Definition
BCP	Business Continuity Plan
IT	Information Technology
RAID	Redundant Array of Inexpensive Disks
ROI	Return on Investment
RTO	Recovery Time Objective
SAN	Storage Area Network
SSL	Secure Socket Layer
VoIP	Voice Over IP
VPN	Virtual Private Network

Chapter 1: Introduction

In the wake of many tragedies which have received national attention, concern has been growing around the effect a major disaster would have on the ability of any organization to function after a catastrophe. Being able to carry on the key business functions of an organization after a disaster occurs requires a great deal of forethought and good management practices, and in the modern world, IT has also become a vital component to the operations of businesses of all sizes.

IT has become so integrated into modern business practices that many offices simply cannot carry on daily business functions without being able to access their information systems or the digital data they contain. In many organizations, if the “computers are down” then productivity plummets if not halts entirely until the systems are online again. Therefore, having systems which are fast and easy to use is no longer enough. Organizations need to also think about designing information systems to be highly available.

Ideally an information system would never go down, but it does happen for a variety of reasons, from human error to hardware failure to major catastrophes. We know that having an information system that is resilient to failures and is also quickly recoverable after a service disruption should be a priority to any organization that values its digital information as mission critical to daily business.

Managing the Business Continuity of IT

Although this concept would seem to be obvious. Through personal experience as a manager in the field of IT, and through years of consultation experience, it is clear that devoting resources to properly preparing for a disaster is not an actual priority for many organizations. Nearly everyone will agree the area of business continuity planning is very important and should be addressed for their organization, but shockingly a high percentage of businesses keep putting it off because it is not pressing or relevant to regular daily business tasks. These businesses claim it will be handled when they have more time or money, but the reality is that this ubiquitous future date usually never comes because there is nothing to stop it from being perpetually pushed into the future.

This report is intended to identify the key aspects of IT that are related to ensuring business continuity after a disruption of service occurs. This is an important issue to all organizations that rely on digital information, and this paper looks at what managers can do to prepare and ensure systems are online quickly after a crisis, and how information systems can be leveraged to make managing a post-disaster environment easier.

Chapter 2: Literature Review

AT&T Inc. 2007. *AT&T 2007 Business Continuity Study.*

This source provides some very interesting and quick facts based on an annual survey AT&T conducts with 1,000 companies in America.

Cisco Systems, Inc. 2005. *Ensuring Continuity of Government Operations*

This is a very informative paper that deals closely with, and focused primarily on, the IT specific aspects of business continuity. It often refers to these aspects as related to government or as they apply to government organizations; however, the content could often be applied to private sector business as well.

Computer Weekly. 2007. *Disaster Recovery and Business Continuity Fundamentals*

The whole point of this article was to point out the benefits of using VoIP services as related to business continuity. It sites several real world examples of stunning endorsements of the technology, but it spends so much focus on hyping VoIP that it does not really spend any time examining the potential negative aspects of the technology.

Comtois, W. and T. Abruzzo. 2006. *Business Continuity Planning 101*

A great down-to-earth guide on what is necessary to include in a BCP.

Elliott, D. and E. Swartz. 2001. *Business Continuity Management: A Crisis Management Approach*

A good collection of information related to BCM which includes some sections that were unuseful, such as historical context and regulatory-related issues. However, it did include a chapter on the “Management of Change” which were an important part of the process often not given enough attention in other sources.

Hewlett-Packard Development Company, LP. 2007. *Impact on U.S. Small Business of Natural & Man-Made Disasters*

This work repeated its statistical points several times and many of its statistical quotes were repeated with statistical quotes measuring the exact same thing but from other sources with different results. This is to be expected in surveys, but they did a poor job of presenting the varying degrees of statistical information they had gathered. Overall though it was a very nice concise collection of information that seemed intended to shock the reader into taking precautions against data loss.

Neidl, L. F. 2002. *Supporting the Public's Business: Continuity Planning & NYS Government*

As the title describes, this work deals with continuity planning for the New York State government, and it goes through its evolution over a twenty year period of continuity planning until after terrorist attacks in 2001. It is a good resource of business continuity planning from an organization that has a lot of experience with the process.

Pereira, B. 2002. *Implementing a Business Continuity Plan*

This article focused too much on the risks specific with doing business in India. However, it provided some excellent graphs and very compelling information on why business continuity planning is not just the CIO's problem, but a problem for the highest levels of management across the entire business.

Rittinghouse, J. and J. Ransome. 2005. *Business Continuity and Disaster Recovery for InfoSec Managers*

This book would be very useful as the title has the words Business Continuity and says it is for "Managers," and even suggests scope related to IT. Instead, this book focuses highly on the type of disasters caused by malicious attackers to an organization's information. Still, the lessons taught are valid for many types of disasters.

Root, D. 2006. *Ensuring Business Continuity in Government*

This publication is designed by Juniper to market the sale of their SSL VPN product solutions to government agencies. However, it does give a lot of valuable information on the functionality and benefits of any SSL VPN solution for allowing remote access versus other technologies. Remote access can be a useful tool in the IT portion of any BCP.

Scholtes, P. 1997. *Leader's Handbook: Making Things Happen*

It is often difficult for an organization that is focused on their daily business to shift focus or add focus to areas which are not directly pressing and which do not directly affect the quarterly bottom line. This book was included to give insight on how to get people motivated and make business continuity planning a priority.

Sikich, G. 2003. *Integrated Business Continuity*

This is a good resource for business continuity information and education. The book is not organized well from a perspective of wanting to know what is necessary for the planning process. However, it is well written and contains valuable information. The language and word choice used by the author carries more impact than many other works in this genre.

Wallace, M. and L. Webber. 2004. *Disaster Recovery Handbook*

This handbook is very good resource which contains a well written chapter about risk assessment. Overall, the book is a good read for anyone responsible or wanting to learn more about the disaster recovery process. However, after the first six chapters, which are universal to the process, the book launches into niche areas not directly necessary to think about for all organizations.

Woodman, Patrick. 2007. *Business Continuity Management: CMI Survey*

This is the compilation of the results of a survey conducted by Chartered Management Institute in 2007. It contains very relevant factual information about the state of businesses in regards to how well, if at all, they have planned for business continuity after a disruption.

Chapter 3: Increasing Motivation for the Planning Process

In order for an organization to respond the most effectively in a post-disaster environment it is important to have a plan of action created before that disaster occurs. The process of creating that plan can seem like a massive undertaking, and this perception is often used as an excuse to stall the process from ever beginning. However, the importance of what is commonly known in the industry as a BCP is recognized as a vital document after a crisis occurs.

Getting started creating a BCP does not have to be a daunting task. The BCP life cycle can be broken down into five manageable areas which can at first be broadly visualized and then later refined and revised. Seeing this plan creation is not a one-time project, but rather a continual process of reviewing, revising, updating, and improving the plan with each succession through the cycle. The milestones of the BCP Life cycle are as follows:



- Analysis
- Solution Design
- Implementation
- Testing and Acceptance
- Maintenance

Figure 1 - Business Continuity Planning Life Cycle
http://en.wikipedia.org/wiki/Business_continuity_planning

Managing the Business Continuity of IT

This process can be viewed on a macro level as simply a few major tasks or steps. However, what can be surprisingly difficult is getting management and employees within an organization focused on actively working on the business continuity planning process. According to an annual survey done by AT&T on large and mid-size companies, even after popular media coverage of terrorist attacks and natural disasters destroying companies, and even after all the hype and fear about potential threats to come, more than one in four companies surveyed still does not have a plan of how to proceed during or after a major catastrophe. And the same study says that 30% of executives in large corporations admit that business continuity planning is not a priority (AT&T, 2007). They are simply too concerned with daily operations of the business to pay serious attention and devote resources to something which is not expected to positively affect the bottom line of the company in the near future.

The reality is that a large percentage of major businesses are run by executives who have judged that it is worth the risk to not make business continuity planning part of their operations, and many who have developed a plan stop what needs to be a continual process after an initial document is created. Failing to continue to review and revise the plan with plan maintenance inevitably results in a worthless plan, as vendors and personnel change and as a business changes in size and scope the plan must change with it, and employees must be continually reeducated enough to know how to execute the plan. These executives who are failing to focus on business continuity are not unaware that others are creating BCPs. Therefore, they are consciously taking a risk they feel is acceptable. Admittedly, it is this ability to take risks safely which likely got

Managing the Business Continuity of IT

many of these people into the positions they now hold. However, gambling with the entire future of an organization and the people who rely on it is not something any executive should do. In fact, executives have been shown in studies that executives have a much higher tolerance for risk when facing threats, than when facing opportunity. (MacCrimmon, 1986). That traditional behavior is not acceptable in the age of digital information. With their actions they are saying, “I don't think a disaster will happen to us” or “I bet we can get by with not devoting resources to this problem until later,” or “The reality of a disaster will never be my problem, because it won't happen while I'm in charge.” But this attitude is very risky for the company's future, since all documents can literally disappear with a single mistake. Managers believe they can control their own environments, but that is not the case anymore, in a digital world one untrained or upset employee, or a single hardware failure, can result in total data loss. 75% of companies go out of business if they experience a disaster and did not have a BCP in place. And that is just for big corporations; a small business without a BCP is nearly as likely to fail after a disaster, except within the first year instead of the first three years, because they lack the resources to “tread water” as they sink (Hewlett-Packard, 2007).

Companies and consumers in the modern world are using technology in many areas of their daily lives. The amount of technological services and the mission critical information necessary to conduct business continues to grow both privately and publicly. Yet the computer systems we use are not 100% reliable. Shockingly, only one in four computer users frequently backup their digital files, even though 85% of those same users claim they are very concerned

Managing the Business Continuity of IT

about permanently losing their important data. That may be expected for regular users and families, but they are just a microcosm of the practices and attitudes of larger organizations. A surprising 40% of small and medium-sized businesses do not backup their data at all (Hewlett-Packard, 2007). This is one of the great benefits of business continuity planning, is it gets businesses to think about how they will recover from a hardware failure or larger disaster. That 40% of businesses have never backed up their data suggests that there is a very real need for businesses to become motivated in adopting business continuity planning into their regular practices.

There is good reason to believe digital information can be permanently lost because, on average, a hard drive crashes every fifteen seconds somewhere in the United States, and 2,000 laptops are stolen every day (Hewlett-Packard, 2007). Also over 30% of personal computer users have previously lost all of their files at least once, and one in five computers has a fatal hard disk crash during its lifetime (Hewlett-Packard, 2007). So, from an IT perspective, a disaster is not just a major event like a hurricane, flood, or an unlikely terrorist attack, but it is anything which may cause an organization to lose its digital information, the very information which has become vital to daily business. Disaster can come in many forms and at any time, and it can happen to anybody. For instance, in 2008, a disgruntled employee for a government office in California locked thousands of employees out of the government's computer system and refused to give them the password. Just because an organization is not located in an area that is not likely to be vulnerable to terrorism or natural disasters is not a justifiable reason to slack on the business continuity process.

Managing the Business Continuity of IT

The chart below shows the reasons that cause companies to lose the data which is vital for the operation of the company. You can clearly see that only 3% is due to hardware destruction caused by any means, including terrorism and hurricanes. This means that even though the driving force for many companies to become involved with the business continuity planning process is due to sensationalized news coverage of disasters, the reality is that companies are 97% more likely to lose access to their data through other means.

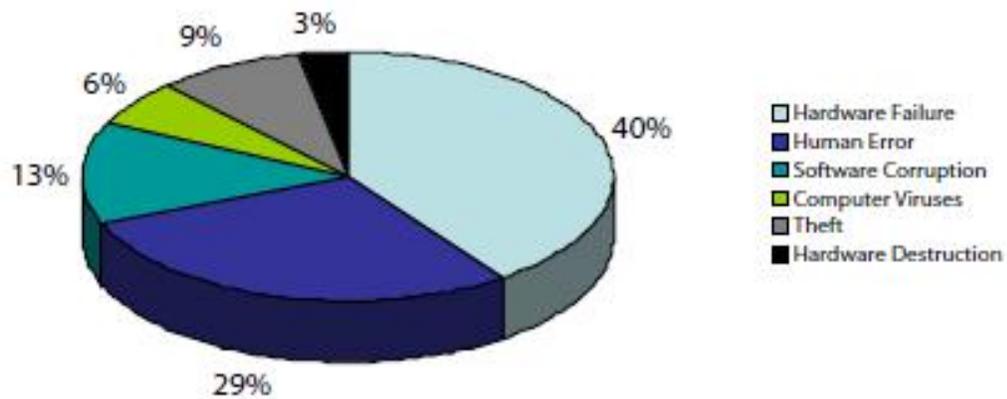


Figure 2 - Actual Causes for Data Loss
http://www.score.org/pdf/HP_Download_ImpactofDisaster.pdf

This means that 97% of the reasons for data loss can happen to anyone, and that only 3% of data loss comes from hardware destruction which comprises all the fear-based stories in the news. If executives are basing their proven tolerance for high risk when it comes to the BCP process against this 3% of sensationalism they choose to ignore, then they are not appropriately accounting for 97% of actual reasons for loss of data. When the driving motivational force only accounts for 3% of the risk, then executives rightfully accept not placing importance on the task as an acceptable risk, but this is the root of the problem

Managing the Business Continuity of IT

for lack of planning, the driving force should be the other 97% of reasons that data is actually lost. This chart's purpose is not to demonstrate the proof that planning for a contingency in case of a sensational disaster is not worth an organization's time, but rather, this chart shows that catastrophic data loss occurs far more often than reasons for losses caused by the sensational news stories, and BCP planning is therefore a much more real problem that needs to be addressed by all organizations who rely on their digital information.

We can think of a company's need to protect its digital information as a large-scale version of our own similar need to protect our individual valuable digital works. From an IT perspective it may seem obvious that everyone prepare for a disaster of information loss. Yet we can see how so many do not even have an old backup copy of any of their data. This is definitely an area where motivation and leadership are needed. Unfortunately many organizations learn to develop good practices through misfortune. However, being proactive pays off, as 94% of organizations who have invoked BCPs for their IT needs claim they have fewer disruptions after creating the plan. So the planning process must in itself have value in identifying areas of operational weakness.

(CMI, 2007)

Chapter 4: Challenges to IT Business Continuity

Business Continuity refers to how an organization will recover its mission critical functions after a disaster or extended disruption. There is a wide range of potential threats to business continuity. Anything may potentially happen, from a natural disaster to a terrorist attack, to internal employee incompetence or sabotage. The very first thing management must do to ensure proper business continuity, is to give this topic the serious and appropriate devotion of resources that it deserves. Most organizations seem to be in agreement that this is a very important area of focus, however even though managers recognize this as being important, they often don't give it the priority it deserves, as it is seen as something that is not pressing.

What is meant by not pressing is a lack of a prevailing attitude that it belongs as an important part of day-to-day tasks and that traditional daily business functions are much more important and real. There commonly exists a disconnect between the realization that planning and preparing for interruptions in business continuity are an important area of concern, yet this is accompanied by an assumption that it can continually be placed on the "back burner". This assumption likely arises from the daily history of business operations. Simply put, yesterday, and last month, and perhaps the entire previous year, there was no need internally to execute the result of such preparations, therefore it is easy to see how this topic can be pushed aside time and time again, until it is actually needed, at which point it is too late. It is common for an organization to recognize the potential threats they face, yet defer dealing with them until some later time, which usually means never. (Redlener, 2006). In fact, 73% of

Managing the Business Continuity of IT

managers report the business continuity planning process is important, yet over half say there is no specific plan in place. Even though news stories of the importance of being able to respond when disaster strikes are covered world-wide, managers often are prone to a fallacy that they can continue to get by without making the planning the recognize as important, into a priority. (CMI, 2007).

Beyond overcoming the mental blockades within a manager's own mind, and determining to devote appropriate resources to coming up with a way to deal with service interruptions. Management may often feel that their staff resources are already busy on existing daily tasks, and that utilizing human resources towards the goal of carrying on good business continuity practices would reduce service and performance levels in other aspects of an organization's duties. However, this is simply a reality of the new business environment. There is no doubt that Information Systems have become an integral part to nearly all organizations, therefore IT has become critical to business continuity, and this new burden which needs continually devoted resources, falls under the management of the IT branch of the organization. Without vigilance, it becomes a one-time project that eventually is forgotten. But in order to effectively implement a plan after a disaster strikes, it needs to be up-to-date and the procedures current in the minds of the people involved in implementing the plan.

Once a manager is committed to pursuing a plan to prepare for business continuity, he or she may often have to rely on their communication skills as a manager to sell the utilization of resources to other members of the larger organization. This is because if no solid BCP already exists or is extremely out

Managing the Business Continuity of IT

of date, then it is very likely that once a new one is seriously being developed, new resources will need to be acquired. The simple fact is that information systems always require computer hardware as a base, and this hardware has long been recognized to have square footage and cooling needs, along with electrical and inter-networking connectivity requirements, as well as competent personnel to install and implement the equipment. In every case, all of these vital components of an information system costs money. If these information systems are truly critical for an organization's mission critical daily business, then at very minimum a BCP must account for how to have these components replicated after they have been completely destroyed. If no plan previously existed or the plan is not up to date, then their very likely is a huge question about where these monies will come from. Generating the funding and partitioning appropriate budget and human resources is a default challenge to getting the process of BCP planning into practice.

Managers of information systems do have several options for continuing business in the face of a crisis. Computer systems are commonly known to occasionally have problems. Workstations often need to be rebooted, and system-wide failures may even occur temporarily when users share centralized systems, and this is common in the industry. The familiarity to small scale "disasters" occurring in the industry is part of the problem when dealing with business continuity in the realm of IT, because these small "disasters" are commonly known in the industry, it is difficult to gain real support for further diligence against a more serious catastrophe. That organizations can and do often recover from more minor disasters; can cause them to falsely believe they

Managing the Business Continuity of IT

can handle any disaster. The users and professionals in the field of IT have become comfortable living with the expectations of a reactionary environment in regards to dealing with problems, and this is a direct challenge to the importance of BCP planning. A small piece of component hardware, or a software related disaster may actually occur on a fairly regular basis for some organizations. However, instead of planning and preventing, they react to the disaster and attempt to counteract it in the shortest time possible using available resources. This is not seen as a major issue to organizations who do not have BCPs. However, it is a component involved in the reasoning that makes it seem acceptable to lack a larger view of a more serious disaster that may affect and entire site or destroy all the computer hardware necessary for operations. These types of disasters are much rarer, but they do happen, they can happen to anyone, and they require good business continuity planning to recover from them.

Traditionally, when systems malfunction, the IT department is left with several options depending on the severity of the crisis and the resources available. An assessment of the problem and estimation of time and other resources necessary for problem resolution can typically be given to management in a short time by their qualified IT personnel. This is known as the Recovery Timeframe Objective or RTO, and in most cases, a service interruption merely means notifying the users that service will be restored quickly and business operations involving the affected information systems are temporarily unavailable. In the event of more serious disruptions, IT departments commonly already have in place two important tools for recovery. One is a good backup of

Managing the Business Continuity of IT

the data, this will be essential to any big crisis, so good practices have already been established in the industry of maintaining reliable backups, preferably off-site. The second is a general idea on how to temporarily carry on business operations without the information systems, even if it's not in writing and means doing things by pen and paper and inputting the data later. However, this only solves the issue of inputting new data. It does not allow the retrieval of existing information until connectivity to the backed up data can be established (Comtois, 2006).

Ideally, modern information systems would be comprised of duplicated components which provide high availability through hardware fault-tolerance. Such systems obviously cost substantially more money. Usually such a system would require complete duplication of the existing hardware, and only combats downtime in case of a hardware component failure. In order to truly be able to respond quickly in case of a massive site disaster, duplicate hardware really needs to already exist at an alternate site, and all necessary software and data needs to be kept up-to-date at the alternate location. This may seem like a huge waste of money, to effectively duplicate the existing IT hardware and software, it may even be seen as an attempt by the IT management to drastically increase the size of their budget. However, that second set of hardware will have to be purchased anyway after a disaster. If the building where an organization's digital data is destroyed, even after retrieving an off-site backup of that data, they would need the hardware to retrieve the data from the backup and to use it effectively in a business environment. Acquiring a duplicate of all existing IT resources "in case" a disaster ever strikes is still a very unrealistic goal for many organizations,

Managing the Business Continuity of IT

and is one of the major challenges an IT manager faces in the BCP process, so alternate methods should be investigated, like the potential to share the cost with a branch in a different region or a mutually beneficiary reciprocal agreement with another business that has similar computer hardware and faces this same challenge.

The final major challenge comes after the creation of the BCP, and relies heavily on personnel. Even with a solid plan and employees who know how to implement it, key personnel may be lost in the event of a tragic disaster, or simply may not be able to be retained after a disaster actually occurs. Providing contingencies for this should not be a factor that is overlooked when preparing for disaster. Personnel loss can range from deliberate reasons from disgruntled employees to selfish or safety reasons of an employee not wanting to clean up the mess or fearing for their personal safety should they return to work after a disaster. It is a challenge of the BCP to address the issue of retaining key personnel, whether through cross-training, bonus incentives, or the plan for temporary retention of outside consultants, appropriate means should be made available to insure the people who are vital for recovery are available during the recovery process.

Chapter 5: Risk Assessment

5.1 – Determining Mission Critical Components

One of the first major considerations when creating a BCP is to identify which systems are critical to the function of the organization. Through analysis of the impact of the Information Systems that IT managers are responsible for, an organization can narrow not only the scope of which systems need quick and reliable replacement, but also give priority to them in the plan. This lends to the discovery of the recovery requirements necessary for each of those critical systems. A result of the analysis phase should be some documentation which details the types of supplies, equipment, and personnel necessary to carry on these business functions, along with contact information for key personnel and consulting organizations which may fill in the gap in the event that key personnel are lost during the disaster.

5.2 – Analyzing Potential Threats

Another key component to the analysis phase is identifying the types of potential threats to your organization. There are way too many potential threats to enumerate them all. But broadly speaking, different organizations may be pre-disposed to different types of threats. Obviously, terrorist attacks are not as real to say a local municipality in rural Kansas as they are to Federal Government buildings or large financial corporations. Likewise, hurricane related disasters are not likely to affect non-coastal areas. Identifying the real potential disasters in your area is important to determine the scope of potential data loss a plan must address. For instance, a local railway may run near your organization's

main data storage area, presenting unique risks such as train derailment into buildings or nearby chemical spills. Identifying the potential disasters which are real for your organization is a key item to planning for them. Some common events, like a single-building fire will likely call for different steps during remediation than large-scale flooding in the region. During this phase, it is important to not only enumerate the different potential disasters, but what broad implications they have to impacting business operations. It is important to remember that this is a cyclical process, so it is okay to initially come up with all potential disaster scenarios, even if sufficient means for remediation are not yet available. This at least gives your organization a starting point, and recognition of weak areas in the BCP offer an opportunity to start working towards proper solutions future cycles of the process can continue to improve.

5.3 – Postulating Threat Impact

Information systems commonly rely on service from privately held telecommunications companies, and in a large scale disaster these services may be unavailable. At least identifying them in the analysis phase, leaves them present to re-evaluate solutions in future reviews of the plan, when monies or other resources may have become available to more properly prepare against the more serious of disaster scenarios. The identification of the potential threats directly leads towards acknowledgement of the impact that can occur due to those threats and gives the initial foundation for working towards obtaining the resources necessary to combat the impact those threats face to the business in a post-disaster environment.

Chapter 6: Designing a Plan for Crisis Mitigation

6.1 – Establishing Plan Goals

The information gathered in the analysis phase can be directly applied to the solution design phase. The important thing to have discovered so far, are the minimum application requirements to carry on essential daily business, and a maximum time frame for how long those applications can acceptably be unavailable. Those two items are essential to the solution design part of the BCP process. The purpose of the solution design phase is to come up with the most cost effective way to meet those two needs.

The solution design phase needs to address the problem of meeting the requirement of reestablishing critical information systems in the time frame necessary, and cover a solution to all the components necessary to make this a reality in a post-disaster environment. As such, it will need to cover the acquisition and activation of computer hardware requirements, space requirements, personnel adept to deliver the desired result to the system users, obtaining and installing software necessary on the replacement hardware, and any other area which will be necessary as a solution to address the issue of having the computer systems unusable for longer than would be acceptable to the organization.

Ideally, a secondary work site could be pre-allocated along with secondary computer equipment and the secondary site could have all necessary applications pre-installed and ready to use, and some form of data replication technology would be in place so that the second site would always be up to date with the current system information. However, this is not always a realistic

possibility in every organization's budget. At very minimum, a reactionary solution should be documented, detailing the requirements for space, hardware, personnel and action necessary, along with key contact information and cost estimates. Then at least an outline would be in place with steps necessary for recovery. In this case money which may not currently be available is saved by not having the expenditure of actually creating a full live contingency; however a framework is established in which significant time is lost between a disaster's occurrence and time to recovery, should a disaster occur. It needs to be the goal of the planning process to establish the current goals of the plan that are the best fit for the organization the plan pertains to.

6.2 – Identifying Critical Personnel

Every organization has critical personnel. This does not suggest that each and every employee is not important to the company, but it does accept the reality that in a post-disaster environment some employees are more important than others. For instance, it is not important to have data entry personnel if the information systems can not be brought online. From an IT management perspective it is necessary to identify who the key players are in getting systems to function adequately enough to implement the BCP. It is a key part of the plan to list out the roles necessary, from hardware experts to network and software engineers, to list names and contact information, and to list alternate personnel our resources to obtain the personnel which are qualified and will be charged with specific tasks which are critical for the operation of the computer systems.

6.3 – Listing Mission Critical Hardware

Just like with key critical personnel, there is a minimum level of computer hardware that must be available for computer systems to function. Physical computer hardware is the foundation of everything a computer system can do, so ensuring the availability of this hardware is another key area of the BCP process. The plan should include detailed information about what systems are currently in place, and generic replacement information on what would be viable replacement hardware should the exact make and model be unavailable in the event of a disaster. If hardware is ruined and inaccessible, then the foundation on which the software of the information systems can run will potentially be an unknown without this component of the plan. Unfortunately not all software is capable of running on just any computer, so listing out the mission critical hardware and having that list available is a key factor in recovery. Valuable time and business revenue can be lost if this information needs to be discovered, so having an inventory of critical hardware is very important.

6.4 – Recording Key Vendors and Suppliers

Not every piece of hardware is readily available at the local computer retail stores. It is common in the industry that the acquisition of hardware and the implementation of software can, and often does, rely on outside vendors. The method for obtaining hardware replacement or assistance with software is not likely to be known outside of the employees who last implemented the current computer system solutions. Therefore, in the event outside vendors or key suppliers would need to be contacted for assistance the most expedient method

Managing the Business Continuity of IT

for doing so would be to have them and their roles clearly identified through this section of the plan. At minimum the plan needs to identify who to contact and how to contact the people and companies they work for, in order to obtain the replacement hardware and software troubleshooting assistance to address problems when they occur. This should include vendors which are necessary for the network connectivity between sites, as the connectivity to the internet and the connectivity to other buildings often runs off network lines leased from an internet service provider, telecommunications company, or other outside vendor. Additionally, agreements with these vendors on their response time in the event of a crisis should be established, along with alternate vendors in the event one vendor is unable to deliver or is likewise negatively impacted by the same disaster. Having the information available, through a BCP, about what vendors are vital outside resources for mission critical applications is a key to the timely recovery after a disaster.

6.5 – Data Recovery Procedures

Having identified the plan goals, personnel, hardware, and key outside vendors necessary to reestablish a working technology infrastructure is still not enough to reach adequate recovery. Procedures need to be documented on how to obtain access to the critical data and software, the critical information necessary for information systems to run, and how to reinstate that data so it is usable by the organization. Who is responsible for retrieval of this software and data and where it is stored, along with a detailed procedure on the steps necessary for this information to become accessible is a vital final part of a plan

Managing the Business Continuity of IT

for recovery. Having all the key personnel and systems available is only the foundation necessary to the actual goal, which is restoring an operating environment which is usable by the business to carry out its critical functions. This section of the plan contains information pertaining to the location of any backup of the data that may exist, what hardware and software is necessary for retrieval, and how to go about doing the retrieval. Once all the information can be obtained, the plan still needs to list steps in this section which identify how to place or install this information onto the systems in a replacement environment and how connectivity can be established to the users of those systems.

Chapter 7: Testing and Acceptance

7.1 – Practicing the Plan

Having accurately identified the necessary elements of the IT infrastructure and services necessary to carry on the business that is mission critical to the organization, and having done due diligence in the creation and design of a solution which would allow for business continuity in a post-disaster environment. The implementation phase is the work of bringing together those aspects of problem discovery and solution design when the time to carry out the solution becomes necessary. In effect, the implementation phase is the true purpose of the BCP, and the test of the plan's effectiveness in the real world.

Ideally, the implementation phase would never need to actually be carried out, as doing so would mean an unfortunate disaster has occurred. However, the simulation of implementation, or practicing the plan, is an important part of the BCP life cycle that should not be dismissed. The act of practice should involve everyone who would be called upon in the event of actually utilizing the plan. Practice involves key players and gets them thinking about whether or not the current version of the plan is the best way to go about things. It is very helpful in the process to discovering what changes need be made, if any, to the current version of the plan. Practicing also helps train key players and keep their roles and duties not only fresh in their minds, but also increases their ability to act quickly in the face of disaster.

Practice should involve testing of the solution to a disaster by running through scenarios using the BCP. Every aspect of the plan that can be reasonably tested should be given due diligence. Just like simulating a fire drill,

the BCP should have appropriate simulation and testing. For instance, having a live off-site backup of digital information is not worth anything if that information is not retrievable. The backup data should be verified and retrieval of that data should be confirmed. Contact phone numbers should be routinely verified to make sure that not only is the information still accurate, but that when a call is made it is answered. The testing and practice of a plan can often reveal many areas in which a plan is weak, along with given a level of confidence in areas of strength.

7.2 – Continuing Education

After involving all the necessary employees and outside vendors in the creation and testing of the plan, the job is not over. Organizations cannot become complacent and forget about the BCP process and go back to business as usual. The BCP process needs to become an ongoing effort within the organization. This includes the continual education and reeducation of employees. If the plan is merely created and becomes a document that sits on a shelf somewhere or that some people vaguely remember being involved with it once upon a time, then should the need ever arise to execute the plan it will not be executed as well as if the key personnel already knew exactly what to do. It is not necessary to maintain a high level of focus, but if several people have left the organization or it has been over a year since the plan has been reviewed, then the plan may no longer be useful. Continuing to educate the members of the organization about the BCP's existence and their role in regards to the plan, is an important part of keeping it up-to-date and keeping roles fresh in people's minds.

7.3 – Gathering Feedback

Simply discovering the minimum applications critical to the organization and designing a solution to keep those available to the system users is not enough to having been considered doing due diligence to the business continuity planning project. The purpose of testing and acceptance is to not only ensure that the solution designed meets the business requirements, but also that the users of information systems within the organization have signed-off that everything they will absolutely need is included in the plan.

Getting the leaders of the branches of the company that are supported by IT to sign off on acceptance of the BCP helps generate positive feedback and constructive criticism. Key players within the organization should sign off on all parts of this project. The end users need to have verified everything they will need has been included in the plan, and also report that the solution appears as if it will work for them. Management of different departments within the organization should sign off on this plan as well. No matter how well thought out and meticulously documented, this plan is ultimately judged by how well its people embrace and execute the plan during a disaster. Requiring signatures will involve more people in the process and increase scrutiny of the document the BCP process produces. Having people more heavily vested in the written plan will ensure they point out areas they think are weak, and it does offer some professional protection to an information systems manager as he or she can not only produce a plan, but show that he had the support of other managers in their sign off of it being a good plan. Although a signature of the manager of the

Managing the Business Continuity of IT

accounting office may not mean as much as the user verification, it does go a long way in showing an information system manager's effort to attempt to create a comprehensive plan. In the event that a disaster occurs and a key component was missing, at least this provides some documentation to the effort of the information system manager to attempt to include all the critical components he or she is responsible for, and that the business would need to continue to function. (Comtois, 2006).

Chapter 8: Plan Maintenance

8.1 – Identifying Plan Weaknesses

After the majority of the work has been done in creating what is believed to be a working version of a BCP, a critical role in maximizing the value of that plan comes in the form of plan maintenance. Part of the BCP process is to review the plan at regular intervals in an attempt to work out any weaknesses in the plan. If there is no immediate way to resolve the weaknesses in a plan, they should at least be well documented so that future successions of plan review can give future reviewers the opportunity to reassess the weaknesses and potentially find new solutions to them. For instance, an organization may recognize vulnerabilities in the way it creates a backup of digital information, but the current budget may be too low to address an immediate solution. Listing out the weaknesses of a plan gives an organization a framework in working towards a more ideal solution as future reviews remind key personnel of the importance to do what they can to minimize these weaknesses.

8.2 – Planning for a Better Plan

The importance of imagination, or thinking outside the box, deserves its own area of special consideration when thinking about all the potential threats that face any organization. For instance, since two-thirds of data loss come in the form of hardware failure or human error, this would be the section of the planning process where an organization should speculate on how that may happen and what can be done to prevent it. The inadequate training or experience of computer technicians could be a factor in human error which destroys the data

arrays responsible for holding a company's digital information. The disastrous consequences that may befall a company who fails to get their head around the issues of hardware maintenance and employee training and devote adequate resources to these areas would likely be more prone than others to a catastrophic data loss event. Planning for a better plan does not simply mean to improve ways to perform better in a reactionary environment after a disaster has occurred, but to recognize and mobilize the means to be proactive in preventing the BCP from needing to be used in a reactionary way. The weaknesses of a plan should be recognized even if they can't be addressed immediately, but so should the structural weaknesses in the areas of business which support prevention of a reactionary plan execution. Planning for a better plan may involve promotion of a currently non-existent off-site backup of digital information, the increase in technical expertise, or even an expressed desire to obtain redundancy in key personnel at some point in the future.

8.3 – Scheduled Plan Reviews

It cannot be stressed enough the importance of scheduled plan reviews. Aristotle once said, "Excellence is an art won by training and habituation. We do not act rightly because we have virtue or excellence, but rather have those because we acted rightly. We are what we repeatedly do. Excellence, then, is not an act, but a habit." That quote should be a great lesson about the importance of making regular plan reviews a habit. Statistically, businesses which have a BCP are much more likely to stay in business after a major disaster if they regularly reviewed their plan, instead of allowing it to fade into the

shadows of the many tasks completed and then forgotten. Businesses change over time in size and scope; their key personnel come and go, as do the technology they employ and the vendors they rely upon. Without regular plan reviews a plan cannot stand up to these changes over time. In fact, 8% of companies who have rehearsed their plans report finding shortcomings during scheduled plan reviews that need to be addressed. (CMI, 2007).

8.4 – Disaster Checklist

The creation of a disaster checklist is a recommended part of the disaster recovery plan. This section merely attempts to concisely express the milestones towards recovery after a disaster has occurred, and serves as a quick guide to the director of post-disaster recovery. The old business cliché that, “time is money” is even truer after a disaster. A major disruption in the ability of an organization to utilize mission critical data systems will likely leave a large percentage of the business’s employees unable to perform their job duties. Sitting down to read through the BCP in its entirety should not be something that uses valuable time before action can be taken. However, if the plan had been reviewed regularly and a checklist was available that identified the milestones to recovery and who is responsible for those areas, then more immediate action can be initiated, leaving the details of the plan divided into sections. The checklist should be concise, and designed to be a cheat sheet that facilitates quick and decisive action towards successful recovery.

Chapter 9: Technologies Which Enhance Business Continuity

9.1 – VoIP

VoIP is a technology that replaces the traditional infrastructure of a company's phone system with a newer design that allows phone calls to travel over the same or similar network as a company uses for their data. There are many reasons a company may switch their phones to use this newer technology, but one of the advantages often overlooked is how it can also be leveraged as part of a company's disaster recovery plan. Using VoIP can allow corporate telephony to be nearly as ubiquitous as other data systems. For instance, it is not necessary to use a particular computer or even be in the building for a user to check their e-mail, where the e-mail data is actually stored is not important as the computer hardware correctly routes the network traffic to where it needs to go. VoIP technology allows this to be done with a business's telephones as well, by utilizing the same internet protocol technology as e-mail. As it becomes more common for companies to use VoIP for other cost-saving reasons, the area of phone systems becomes more and more the responsibility of IT managers. Leveraging existing VoIP technologies, or incorporating the desire to obtain VoIP technology into the disaster recovery plan should not be overlooked. The ability to make and answer telephone calls on the company's normal phone numbers from anywhere with an internet connection is an amazing feature of VoIP that is not likely utilized on a regular basis, but certainly can be a big benefit in the event of a disaster. VoIP needs to be the core of any well-planned communications recovery strategy for a major disaster, and companies can get a higher ROI

(ROI) from their VoIP implementation if they use it to bolster their disaster recovery plans. (Computer Weekly, 2007).

9.2 – Remote Access

Remote access is any means in which employees of a business can access their digital information and do their work without having to be physically at their desks. Many organizations allow employees to work from home as a benefit that allows them more time for a family life, reduces the gasoline and other transportation costs to employees, and can even reduce the square footage necessary for a business to house workers on-site. VPNing or VPN technologies allow employees the ability to access their information from practically anywhere, turning their home computers into computers capable of acting as if they are at their desks on the corporate network. Some smart phones even allow their users to remote control work computers to check e-mail and edit spreadsheets. The decentralization of employees inherent in the ability remote access provides, could allow them to keep working even if the entire building they normally work at is quarantined or even completely destroyed, and allowing some people to occasionally work from home could not only save key personnel in a major disaster, but could save lives.

9.3 – Hosted Services

Hosted service providers are outside vendors which can delivery traditional IT functions over the internet. There are many benefits to using hosted services which may or may not be right for a particular organization. However, they do

Managing the Business Continuity of IT

offer a clear advantage of decentralization over traditional in-house IT solutions when perceived from a disaster recovery perspective. By using a hosted service a business may be able to outsource their data storage, websites, or e-mail servers to another organization which promises connectivity to those applications from any computer which has an internet connection. If your company only has one building or the funds to create one server for a mission critical function, then that is putting a lot of faith in that one server always operating successfully and being available. A hosted service may on the other hand have servers all over the world which would allow a business to retain access to their applications even after an entire city was destroyed. For this reason, utilizing a hosted service should not be overlooked. Even just as contract with an outside organization to securely store a backup of a company's digital information could prove to be the difference between total destruction of a company and resilience in the face of a catastrophe.

9.4 – Clustered Services

Clustered services can be thought of as in-house hosted services. Clustering technology allows the grouping of multiple computer servers to function as a single server. This is definitely a great safeguard against the single point of failure that is reliance on a single server computer, and does not have the inherent risk of exposing sensitive information to outside organizations that contracting with a hosted service would have. The downside of clustered services are the increased cost of obtaining one or more duplications of your

existing computer server hardware, along with an increased complexity that requires a better trained IT workforce.

9.5 – Wireless Networks

Wireless networks are another component which may make disaster recovery easier. A sewage pipe bursting and causing the evacuation of a floor normally used for business would leave several employees displaced from their desks. Getting them back “on-line” would traditionally require running network cables to new locations, but with wireless networks this would be unnecessary. Some cell phone carriers are now coming out with high-speed wireless networks that can function on their cell service, so that a computer can have access to the internet and potentially to corporate data as long as the computer is within cell phone range. Continuing to examine the area of wireless technologies with each plan review will likely soon open up new opportunities to create a better BCP. The ability for a company to do business instantly from any temporary office space is certainly a huge advantage in time savings, and wireless networks can provide this in some areas, with increasing coverage every year.

9.6 – RAID and SAN Usage

Redundant arrays of inexpensive disks or RAID, and SANs or SAN, are information technologies which employ the use of multiple hard disks acting as a single disk. The advantage is that they provide high availability to data. If all information is stored on a single hard disk and the hard drive “crashes”, then all information stored on that disk is unusable. The disk would have to be replaced

and hopefully the data could be recovered from a backup. However, during recovery the data would be unavailable. However, with RAID and SAN technologies it is possible for a hard disk to stop working, or even for multiple hard disks to crash, and for the disaster to be transparent to the user of that data. Computer operators can then remove damaged hard disks and replace them without data loss or downtime in accessibility to the data. Since most data loss disasters come from hardware failures, and a hard drive dies somewhere in the United States every fifteen seconds, this technology is arguably the most important in preventing an IT disaster.

9.7 – Off-site but Not Off-line Backups

Thinking outside the box with backup solutions has many benefits. Traditionally hard disks were expensive and in order to retain backups of company data, tape drives were and still are the most common means of backing up data. However, tape backups have inherent problems. Tape is more prone to recovery failures than storing information on hard disks, and time to recover from tape can take hours or even days, as every file must be copied from tape to hard disk. However, if a business were able to backup its data to a computer in another building then this data could be easily switched to become the copy employees use, should the normal server be destroyed or inaccessible the time to recovery can often be reduced by several hours by utilizing online backups of data. The number of backups whether offline or not, directly increases the cost to a company's disaster recovery ability, but it also directly increases the chances of successful recovery. Most data loss scenarios are recovered from through

Managing the Business Continuity of IT

means of some form of backup, so having a reliable backup that is verified to be viable should be the cornerstone in any disaster recovery plan.

Chapter 10: Conclusion

Developing good practices in regards to business continuity planning is essential to curbing the serious threat to the survival of a business in the modern digital world. Core functions of business rely on technology more and more every year, while an inappropriately small amount of concern has actually been placed on safeguarding this digital backbone that modern business needs to survive. While no business can become 100% resilient to all disasters the ability to be resilient for most disasters needs to start with giving proper priority to planning for disaster scenarios.

This field project provides the basic tools necessary to increase awareness and motivation for the disaster planning process, and a basic framework that makes approaching the creation of a BCP for safeguarding a company's digital information a less daunting task. Applying the basic principles of the five stages in the business continuity planning life cycle will help any organization mobilize an effort to create a BCP or improve an existing plan. It is often said that, "failure to plan is planning to fail", and that has been witnessed time and time again as company's continue to increase their reliance on technology at a far greater pace than they give due diligence to prevention of data loss.

References

AT&T, Inc. *2007 AT&T Business Continuity Study*. 2007.

http://www.att.com/Common/merger/files/pdf/business_continuity_07/US_Survey_Results.pdf (accessed September 06th, 2007).

Chartered Management Institute. *Business Continuity Management*. 2007

http://www.preparingforemergencies.gov.uk/business/bcm_report2007.pdf

(accessed September 06th, 2007).

Computer Weekly. *Disaster Recovery and Business Continuity Fundamentals*.

2007. [http://www.computerweekly.com/Articles/2007/08/07/226101/disaster-](http://www.computerweekly.com/Articles/2007/08/07/226101/disaster-recovery-and-business-continuity-fundamentals.htm)

[recovery-and-business-continuity-fundamentals.htm](http://www.computerweekly.com/Articles/2007/08/07/226101/disaster-recovery-and-business-continuity-fundamentals.htm) (accessed August 08th, 2007).

Comtois, W. and T. Abruzzo. *Business Continuity Planning 101*. May 26th, 2006.

<http://www.securityinfowatch.com/article/article.jsp?siteSection=392&id=8284>

(accessed March 13th, 2007).

Coop Systems. *Business Continuity Program Management Tools: Combining*

the Power of Business Continuity Management and Emergency Notification,

2005.

http://www.idsemergencymanagement.com/Common/Paper/Paper_134/Business

[%20Continuity%20Program%20Management%20Tools.htm](http://www.idsemergencymanagement.com/Common/Paper/Paper_134/Business%20Continuity%20Program%20Management%20Tools.htm) (accessed

September 06th, 2007).

Managing the Business Continuity of IT

Department of Homeland Security. *Preparing Makes Sense: Get Ready Now!*

U.S. Department of Homeland Security, 2005.

Elliott, D. and E. Swartz. *Business Continuity Management: A Crisis*

Management Approach. Taylor & Francis, Inc, 2001.

FEMA. *Public Assistance Guide*. FEMA, 2001.

FEMA. *State and Local Mitigation Planning: Understanding Your Risks,*

Identifying Hazards and Estimating Losses. FEMA, 2001.

Hewlett-Packard Development Company, LP and SCORE. 2007.

http://www.score.org/pdf/HP_Download_ImpactofDisaster.pdf (accessed June 21st, 2008).

Juniper. *Ensuring Business Continuity in Government*. September, 2006.

http://www.juniper.net/solutions/literature/white_papers/200203.pdf (accessed March 15th, 2007).

MacCrimmon, K. R. and D. A. Wehrung. *Management of Uncertainty: Taking*

Risks. New York, Free Press, 1986.

Managing the Business Continuity of IT

METAgroup.com. *Ensuring Continuity of Government Operations*. February 2005. http://www.cisco.com/web/strategy/docs/gov/agencies-defense_MetaGroup.pdf (accessed March 15th, 2007).

Network Magazine. *Implementing a Business Continuity Plan*. 2002. <http://www.networkmagazineindia.com/200208/cover1.shtml> (accessed March 13th, 2007).

Nudell, M. and N. Antokol. *Handbook for Effective Emergency and Crisis Management*. Lexington, Massachusetts, Lexington Books, 1988.

NYS Forum. *Supporting the Public's Business: Continuity Planning & NYS Government*. December 2002. http://www.nysforum.org/documents/html/whitepapers/bcp_white_paper.htm (accessed March 14th, 2007).

Posner, R. A. *Catastrophe: Risk and Response*. New York, Oxford University Press, 2004.

Redlener, I. *Americans at Risk: Why We Are Not Prepared for Mega-disasters and What We Can Do Now*. New York, Alfred A. Knopf, 2006.

Rittinghouse, J. and J. Ransome *Business Continuity and Disaster Recovery for InfoSec Managers*. Elsevier Science & Technology Books, 2005.

Managing the Business Continuity of IT

Scholtes, P. *The Leader's Handbook: Making Things Happen, Getting Things Done*. McGraw-Hill Companies, 1997.

Schwartz, J. A. and P. D. Cynthia Barry. *Emergency Preparedness for Correctional Institutions*. Kansas Department of Corrections, Letra, Inc, 1982.

Sikich, G. *Integrated Business Continuity: Maintaining Resilience in Uncertain Times*. PennWell Corporation, 2003.

Wallace, M. and L. Webber. *Disaster Recovery Handbook: A Step-by-Step Plan to Ensure Business Continuity and Protect Vital Operations, Facilities, and Assets*. AMACOM, 2004.