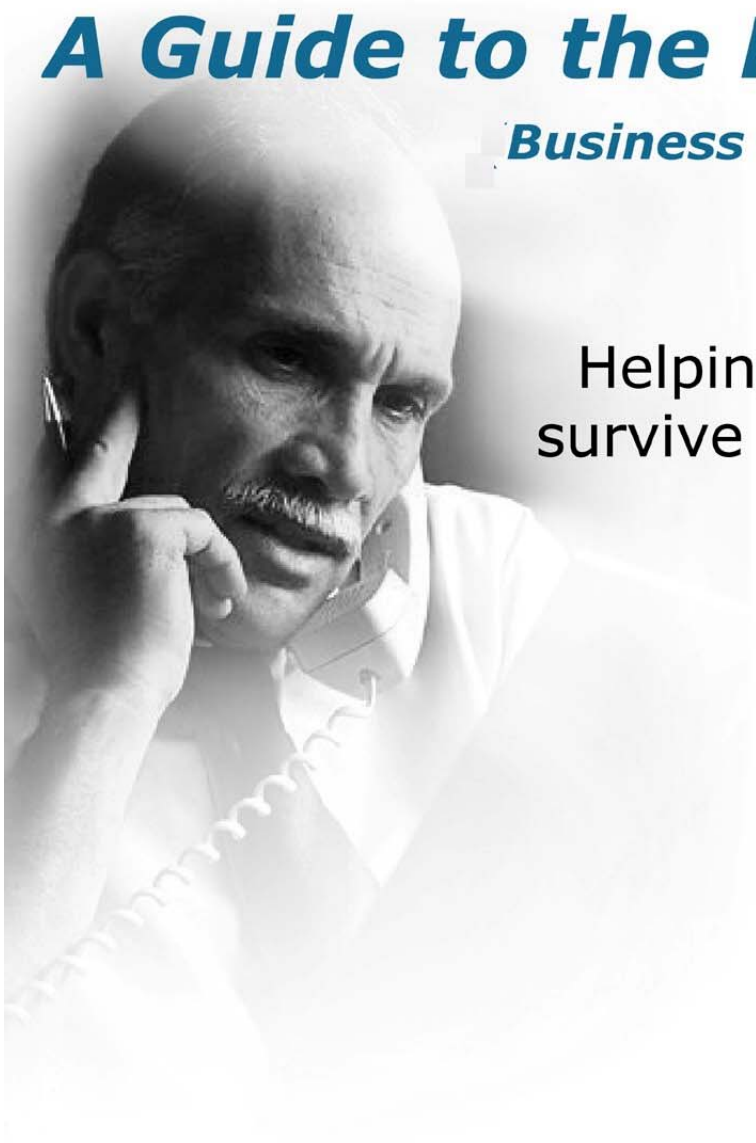
A Guide to the Perplexed

Business Owner



Helping your business survive the unexpected shutdown

Edited by Eric Beser
CEO ennovate inc.
eric.beser@ennovateinc.com

ennovate inc.

Protecting the economy One Business At A Time

A GUIDE TO THE PERPLEXED BUSINESS OWNER

HELPING YOUR BUSINESS SURVIVE THE UNEXPECTED SHUTDOWN

Edited By Eric L. Beser

CEO, ennovate inc.

Eric.beser@ennovateinc.com

Table of Contents

Forward

Being prepared for a rainy day is natural. As individuals, we have a plan ready to put into play for all those "in the event of" situations… traffic jams, a flat tire or even a bad storm. But what about your business? Have you taken the time to plan for an unexpected event that may affect your livelihood?

If you are like most, the answer is probably NO! And, this unforeseen, unexpected event can result in catastrophic loss to you and your business. This is not a scare tactic but a smart business standard. Take a close look at how prepared your business is for that "what if" situation.

An ounce of protection – the Ennovate way.

The key to being prepared is to have a comprehensive business continuity plan. This plan is a proactive, systematic approach complete with a safety net and steps to keep your business productive and profitable.

Ennovate Inc. helps businesses plan for, survive, and prosper in spite of unexpected shutdowns. We do so by helping our clients identify the risks that their businesses face, and also by proactively providing alternatives to follow should the unexpected shutdown occur. We make the shutdown "expected" and "planned for," thus reducing the cost if and when the shutdown occurs. The events of September 11th and the ensuing Anthrax bio-terrorism gave "Business Continuity" new meaning. Although the probability of these events occurring again is quite low, business owners recognized the need for Continuity planning. The question, "What if you had to leave your office within 30 seconds and could not come back for a month, if ever?" would be asked again and again. We found that, even in the aftermath of Sept. 11th, this question remains answered with only a shrug. Business owners, who normally would not think twice about purchasing liability or health insurance, reply with a fatalistic, "I will deal with that if it happens."

There are several problems with the business owner's view of Business Continuity. There is a false sense of security in thinking that Continuity is an Information Technology problem. Computer backups, though quite reliable, will often fail. We have seen some outstanding Information Technology recovery plans created by top professionals. However, an audit and review of the plans reveal possibilities of failure because the developer saw the business from the Information Technology perspective, and failed to see all the dependent business processes. Failure in any one of the business processes causes the business to shut down. Business Continuity is part information, part logistics, and part business processes. To complete a full continuation plan, it is important to look at all three areas.

This guidebook is a compilation of knowledge from our consultants and other leading consultants in the field of Business Continuity. The guide is not designed to train Business Continuity professionals, but rather to inform the business owner of what is necessary to help their business survive unexpected events. The small business does not have an Information Management department, nor does it have many business processes for which to account. However, the small business is the most vulnerable to unexpected shutdowns because it cannot sustain a cash flow interruption, or lost customers, for any length of time.

Although the body of literature in the field of Business Continuation suggests that Continuity Plans are best designed by skilled professionals, a small business that cannot afford the professional may view this guide as the closest thing to a business continuation plan. Acute planning, awareness of

the risks, and knowledge of the common forms of shutdowns that may occur can save the small business from extinction.

To the business owner who reads this guide, the benefits will be apparent. The goal is to save money and to preserve wealth. Other benefits include:

- Discovering what risks need to be avoided immediately
- Closely examining processes, policies, and procedures to ensure requirements are met
- Developing an awareness of what processes actually impact the business
- Developing an appreciation of the business continuation plan as an integral part of the business plan

Who needs a plan? Every business needs a plan. No questions asked. Any business that can lose $1000 or more per hour during an unexpected shutdown needs a plan to minimize the loss if that shutdown does occur. One contributor, John Glenn CRP, writes:

Business Continuity, as with most other professions, is one of never-ending education. Planners as a group are willing to share their experiences so we can gain from others' knowledge rather than learn at our Clients' and Employers' expense. Knowing that no plan is perfect and that we can never plan for every contingency, we still go forth making a best effort. As you read through this book, keep in mind two visual aids that should be before all Business Continuity planners:

- *Rodan's Thinker being taken out of a shipping crate*
- *A household vacuum cleaner*

Why these visuals? Because, as you will learn in the following pages, a successful Business Continuity planner must

- *Think outside the box*
- *Can't work in a vacuum*

It may be corny, but it is true.

I want to thank the contributors who emailed their tips, techniques, and articles, as well as those authors who contributed whole sections of this guide. Editing became a challenge because of the overwhelming amount of useable material that arrived. These business continuity consultants are a dedicated bunch, all sharing a wealth of knowledge from years of experience in the field.

THIS GUIDE IS AVAILABLE AS A DESKTOP REFERENCE. SIMPLY GO TO http://www.expertpractices.net AND GET THE DOWNLOAD INSTRUCTIONS FOR THIS REFERENCE. IT'S SEARCHABLE, AND EASY TO USE. AND WILL BE UPDATED EVERY COUPLE OF MONTHS.

About This Guide

The Guide to the Perplexed Business Owner is created for a wide range of businesses that can benefit immediately from the practical knowledge of keeping your business thriving in spite of unexpected shutdowns.. Staying in business today requires more than delivering a high quality or service. Most business owners and executives struggle daily with increasing productivity and profitability while managing bottom line expenses. Our goal is to give you concrete tools that will help you reach your business goals – and help you focus on your core competency -- instead of spending countless hours or days coping with an unexpected business shutdown.

This guide was made possible by the generous contributions by renowned experts in the Disaster Recovery and Business Continuity fields. We have also provided links to these experts and other essential tools that will help you build your own business continuity plan and library of resources. At the very least, we hope you will gain essential knowledge and tools that will keep your business up and running.

How to Share This Guide

We encourage you to share this guide with colleagues and friends and have included instructions on how to pass-along the guidebook via email. For a free desktop reference version of this guide, simply go to www.expertpractices.net and file out the request form. You will receive automated instructions on downloading a searchable, easy to user, desktop reference copy.

The Guide to the Perplexed Business Owner is available in several easy-to-download formats: Adobe PDF, e-Book desktop reference, and Microsoft Reader (coming soon).

Updates

This guide will be revised five times a year. This is release 1.0. By registering as a Guide reader you will be notified via email of a newer release. We will be adding additional tips, techniques, articles by experts, and strategies to follow. Please register yourself as a user.

Sponsors, Licensing and Copyright

Please contact us if you want to be listed in the guide as a service provider, page sponsor or book sponsor. Have your message shown to over 1.2 million readers.

License the guidebook for immediate mass distribution to your organization or customer base by contacting the editors directly at sales@ennovateinc.com abd see how to co-brand this booklet. There is no charge for this service, however there are certain guidelines that need to be followed.

Contact Ennovate Directly

For more information on Ennovate's services or how we can help you develop your Business Continuity Plan, contact us toll-free at 1.866.366.6842 or via email at sales@ennovateinc.com or visit us on our website at www.ennovateinc.com for more information

Introduction

According to the Gartner Group, a major-market research firm, fifty-percent of all businesses fail after experiencing a major disruption. Lack of planning for these disruptions can cause a business to lose a majority of its customers. A business is more likely to recover if it has a plan and has taken into account all of the areas on which it depends to function normally. It is difficult to predict the failure of something on which a business depends.

Unexpected shutdowns occur for a variety of reasons.

Case: You arrive at the office and turn on your computer, and, instead of the prompt that indicates Windows startup, you see "C: Hard Drive Not Recognized." The hard disk has just failed, along with your data, operating system, and applications.

Case: While at Airport Security, you place your laptop on the conveyor belt, but before you go through the metal detector, someone in front of you causes the detector to sound off, effectively stopping all traffic through the detector. By the time you get through the detector, your laptop is gone.

Case: Your office is over a restaurant, and the kitchen fire has just caused significant damage to the building. You cannot use your office until the fire safety inspector and building inspector have decided that the building is safe.

Case: Your telephone provider has decided to shut down due to Chapter 11 or Chapter 7 Bankruptcy. Your phone system no longer functions, and Verizon, Quest, AT&T, SBC, or PacWest have stated that it will be forty days or more before you can be hooked up and back in service. Your phone number states that you have been disconnected.

Case: Your Internet Service Provider (ISP) has ceased operation with only one-week notice. You no longer have a network into your office. A new ISP states that it will be fifty days or more before a new T1, DSL, or Fractional line is connected in your office.

Case: (This actually happened in Baltimore.) A train carrying chemicals derails in an underground tunnel under the city. The fire in the tunnel causes a water main to burst. The fire department blocks entrance to your office building, and in fact, your building cannot be used for 6 days.

Case: (This is an old one, but still good.) It's 2:00 AM and its tax season. You have just completed a series of tax returns for your customer. As customary, you save all data on a floppy disk. After putting a floppy in the disk drive, you type what you think is "Format A:" and several repeated carriage returns to begin formatting the disk. It's late and you take a brief break while the disk is being formatted. When you return, you realize that instead of typing "Format A:", you have typed "Format C:", have skipped past all the safety checks, and have happily formatted your C drive.

With the exception of the kitchen fire and the train derailment, the probability of these shutdowns occurring regularly is quite significant. In fact, most computer hardware, in consistent use over a period of three years, stands a forty-percent chance of having a catastrophic hardware failure. Most small business owners purchase non-brand computers, disregard repair policies (they figure they can throw the computers out and purchase new computers at the same price), and depend on these non-brand computers heavily. Most use floppy disks, an inexpensive file server, or a cheap tape drive for backup. Rarely are the backups tested to determine if a system can be rebuilt from scratch, and many times, the backups fail to restore critical data.

Each of these unexpected shutdowns carries with it a cost to the business that translates into lost time, lost customers, and lost opportunity. An unexpected shutdown is defined as an event that:

- Affects physical facilities or environment
- Affects health, safety, or welfare of personnel or general public
- Affects Business Operations

Shutdowns may be classified as malfunctions, disasters, or catastrophes. The probability of a letter arriving laced with Anthrax or an airplane flying into the building is quite low. However, more likely events, including storms, tornadoes, electrical problems, earthquakes, flooding, snowstorms, and fires, occur less frequently than hardware failures. Yet these events still occur frequently enough to be a concern for most people.

The purpose of this guide is to help business owners understand how to plan for unexpected shutdowns, survive them, and continue to prosper. Although the aforementioned unexpected shutdowns (with the exception of the kitchen fire and train wreck) all deal with computers or equipment, we will look at business continuation as more than an Information Technology (IT) problem. The problem with most guides to business continuity planning is that the shutdown is treated strictly as an IT problem. Most white papers deal with remote data centers, hot sites, cold backups, domain switching, etc. True, even for the smallest of businesses, data is everything. But the small business has no IT department and may only have one person, or a contract with a service, that truly understands IT. For the most part, however, computers are treated like appliances, and when an appliance breaks, it is repaired or replaced. Because most papers on Business Continuation deal with IT-related issues, the small business sees Business Continuation as an IT problem. Since the early days of PCs, the act of backing up data has been drummed into the most naïve of businessmen. Only the brave soul would continue to use a computer without ever doing a backup of critical documents or files needed to conduct business. Since most people do regular backups, they are lulled into a false sense of security, thinking that they have a plan in case something happens to the computer.

We have a plan to help. In fact, we have software that you can download and install which will do remote backups of up to 4GB of critical data on your computer for only $14.95 per month. There are vendors with whom you can pre-arrange replacement computers.

We have simple techniques to follow to ensure that your data will be there even when your computer is not.

Most business continuation-consulting firms ignore the small business. There is not much consulting opportunity when there is no IT staff, only three or four people in the business, and a handful of PCs. This customer would not pay for, nor could they afford, the high-priced agency that produces a top-notch plan to continue the business. Yet these businesses are the most vulnerable to unexpected shutdowns. The point of this guide is to provide the expertise from Ennovate Inc.'s consultants, and from other top consultants in the field who have years of experience, to help the small business plan for, survive, and even prosper in spite of the unexpected shutdown.

In the chapters that follow, we will look at the various types of unexpected shutdowns and suggest risk-reducing techniques. Some of our suggestions come from consultants working in the field. Each risk will have a series of activities that can be used as a plan for what to do should the unthinkable occur. In addition, some of these risk mitigations will contain names of consultants who can handle data restoration, repair PCs, restore offices after fires, and do cleanup after floods. Yes, we will show you some IT tricks too. We will show you some software to remotely back up your

critical data in real time, as it changes, to reduce the amount of time it takes to compete a data backup. Other simple software produces images of operating systems to reduce the time that it takes to restore a system to operation. We will introduce you to some concepts that are key to preparing oneself to handle any type of unexpected shutdown. At the very least, this guide can show you how to complete a business continuation plan, and there will be places where you can fill-in names and contacts for your specific business activity. ***It is important to note, however, that this guide is just a guide, that continuation plans are personal and unique, and that continuation plans should be done by professionals who know what they are doing. Ennovate cannot take responsibility here if something is missing from your plan.*** Please feel free to call us, or any other professional listed in this book to review your plan, and perhaps to do a proper risk analysis and business impact analysis on your business. Ennovate has audits varying in complexity (and price).

SEND THIS GUIDE TO YOUR FRIEND. YOU CAN CLICK HERE TO GET TO OUR WEBSITE, http://www.expertpractices.net, TO SEND DOWNLOAD INSTRUCTIONS VIA EMAIL TO ANYONE WHO YOU THINK WOULD BENEFIT FROM BEING PREPARED TO FACE UNEXPECTED SHUTDOWNS. WE WILL UPDATE THIS GUIDE EVERY QUARTER TO INCLUDE NEW TIPS AND TECHNIQUES TO MITIGATE BUSINESS RISKS. SIGN UP FOR A DAILY EMAIL, A WEEKLY SUMMARY, OR A MONTHLY STRATEGY OF TIPS AND TECHNIQUES FROM EXPERTPRACTICES.NET.

Chapter 1 What is Disaster Recovery?

THANKS TO ANDREW VESAY – SOLUTION ARCHITECT FOR ROCKEFELLER GROUP TELECOMMUNICATIONS SERVICES.

Today, more than ever, we have a heightened awareness of potential dangers that exist in everyday life. As a result, the business world is seeing a dramatic increase in the need to address Disaster Recovery as a critical aspect of daily operations.

So, what is "Disaster Recovery?"

Disaster recovery is simply planning ahead to avoid problems, and being prepared in the event a problem occurs. Disaster recovery is not something you can hold in your hand. You cannot go to the store and buy disaster recovery. There aren't any magic Disaster Recovery do-it-yourself kits available on the Internet. When you think about it, most people are exposed to Disaster Recovery strategies in daily life, not under such an imposing title. Some of the commonplace Disaster Recovery includes:

- Spare tire in the trunk of the car
- Yearly flu shot
- Emergency exit signs
- 911 Emergency support services

Each of these examples illustrates an aspect of planning ahead or responding to everyday problems. Disaster Recovery for business is used for the same objectives. From a business perspective, Disaster Recovery has three basic components referred to as:

- Business Planning and Preparation
- Business Systems and Technology Preparation
- Incident Response Planning

Just as our everyday measures protect us from potential hazards, these business-related components of Disaster Recovery address how to effectively prepare for and respond to unexpected shutdowns. You can compare the three components of Disaster Recovery for business to the spare tire in your trunk:

- **Planning and Preparation:** What steps do you take to ensure you are prepared?
    - Because you drive through the nail factory everyday, you should keep a spare in the trunk.
    - Check the spare tire each time you check your oil to make sure it is still there.
    - Keep the spare tire-changing manual in the glove box, and make a "dry run," practicing changing the tire in the driveway.

- **System and Technology Preparation:** Do you have the tools you need in case of a problem?
    - Is the spare tire inflated?
    - Is the spare tire the correct model?
    - Can you get another spare if this one doesn't work?
    - Does the jack work?
- **Incident Response Planning:** You've got a flat tire! What do you do?
    - Follow the spare tire manual; you change the flat with the spare.
    - You proceed to the nearest service station, as stated in the manual, to have your primary tire repaired.
    - You replace the spare with the repaired primary tire.
    - You re-check the spare and place it back in the trunk for the next time.

In a nutshell, this is Disaster Recovery strategy. While the technical and logistical aspects of Disaster Recovery can be very complex, the operational components can be boiled down to three basic concepts:

- Do you know what your risks are?
- Are you taking the necessary steps to proactively prepare for potential problems?
- Do you have a plan identifying how to respond when a problem occurs?

Scouts provide a prime example of a Disaster Recovery strategy in their simple, yet effective slogan, "Be Prepared!"

How do you know your Disaster Recovery Plan will work? To perform a rudimentary assessment of your organization's Disaster Recovery capabilities, you need to answer (honestly) the following three questions:

- Do I understand all of the systems and processes that are critical to the operation of my business?

Solid Disaster Recovery strategies must be based on quantifiable facts, not on assumptions and opinions.

- Do I have a prioritized plan to recover each system or process?

While it may be easy to say that "everything is important," when a dollar amount for recovery is applied to specific business functions, many aspects of a business drop down or off the priority list for Disaster Recovery solutions.

- Will my plan work? (This is the toughest one to answer honestly)

One of the biggest mistakes in business (some times career-ending mistakes), has been working with a Disaster Recovery solution based on "I think it will work," as opposed to "I know it will work." Until you have performed a test of your Disaster Recovery plan, there is no way to know that it will work.

Many professionals will answer no to at least a few of these questions. How many can say they truly understand and have performed a formal review of all aspects of their business, created a list of the critical business functions, and prioritized them from the most critical to the least?

A comprehensive Disaster Recovery solution encompasses ongoing assessment of risks, implementation and updates of business processes and technologies, and regularly scheduled testing and review of Disaster Recovery Plans.

Advice from the field:

We regularly test Disaster Recovery Plans by asking participants to take over roles or replace key employees in testing out functions. For example, we ask the Chief Financial Officer of the company to describe how to restore critical data on a computer without asking the Manager of Information Services how to proceed. The assumption is that part of the team has been removed suddenly. It's important that each member of the team understand all the critical processes that are called out in the Disaster Recovery Plan.

A good opportunity to test a Disaster Recovery Plan is when the company is moving or changing locations of key computing systems. The Disaster Recovery Plan can also be used to handle moving and relocating critical resources. It's a good opportunity to test backup and recovery procedures for computing.

Chapter 2 Business Risks and Their Impact

Business risks come in all sizes, shapes, and impacts. The trick in surviving these risks is to plan accordingly and create mitigating actions in case a shutdown risk actually occurs. Not all risks will occur to a given business. Some risks, such as earthquakes, have a low probability of occurrence unless you live in a specific area, like California. Tornado risks also have a low probability in areas that are not prone to sudden weather changes. Snow emergencies rarely occur in Atlanta, GA (when they do, driving is an interesting thing to watch), and the risk of civil disturbance may never occur in rural areas. Not all risks need to be planned for, nor should they be included in a Business Continuity Plan.

Risk mitigation is not an IT problem. Risk mitigation is about logistics and operations. Risks occur all the time. To defend against risks, you perform actions that reduce the impact of a risk. That's what mitigation is all about. Countermeasures are preventative actions that reduce the impact of risks when they occur.

The first step to surviving unexpected shutdowns is to do a study on what risks can occur to your business and to determine the probability of these risks occurring. This study is called an operational risk analysis and is important in determining what risks are significant to your business and what risks may be safely ignored. In an operational impact analysis, each potential risk is examined. A determination is made if this risk can actually occur and if it does, what the monetary impact on your business really is. Generally, when a risk is low, or there is no financial impact if a risk occurs, then it may be safely ignored. Additionally, if a risk probability is high, and you already have a plan to conduct business should that risk occur, then the risk may be ignored as well. You have already planned to mitigate the risk.

This chapter will look at all sorts of business risks in order to catalog them and suggest countermeasures to reduce the impact of these risks. The Business Continuation Plan is nothing more than a catalog of countermeasures for your business, in order of occurrence probability. Unexpected shutdowns occur in the following areas:

- Risks that affect physical facilities or environment
- Risks that affect health, safety, or welfare of personnel or general public
- Risks that affect Business Operations

Planning for all risks is a costly and time-consuming process. Large businesses have teams of individuals that are specifically trained to look at all these operational risks, building and testing Business Continuation Plans that are volumes in length. These businesses survived Sept. 11 because the IT department had planned remote data centers, having the ability to switch systems within minutes. Many businesses in the World Trade Center were back in operation hours after the buildings came down. Many financial services lost only a few transactions and resumed operations in hotels with Internet connections. They had contracts with alternative facility providers, had data centers that were switched to provide continuous service, had tested backup plans, and had personnel plans that allowed employees to work at home. These continuity plans took weeks and months to develop and cost significant dollars to create.

The small business has little resources to develop complex continuation plans. They have little flexibility when shutdowns occur. According to a report in the New York Times, 45,000 small

businesses ceased to exist on Sept. 11. They could not sustain the operational impact of being in or around Ground Zero, or, because of some logistical tie to the World Trade Center, could not sustain the loss of income.

Would your organization be able to recover from an unexpected shutdown, such as a computer failure or theft? Could this recovery be substantiated? The *Executive Scorecard* shown below offers a quick measure of your small business's readiness for this type of shutdown.

#	Executive Scorecard	Yes	No	?
1.	Do you have a written Business Continuity Plan?			
2.	If so, have you fully tested it?			
3.	If tested, did you pass your test?			
4.	Have you quantified and ranked the business and financial risk of outages to all vital functions?			
5.	Are you prepared to address liabilities and fiduciary responsibilities in case of disaster?			
6.	Are business continuity plans kept current and updated for business changes?			
7.	Do you perform back-ups faithfully and include every server and hard disk?			
8.	Do you regularly send your back-ups to a safe, off-site archive?			
9.	Have you standardized on a proven media, drive, software, and automation back-up solution?			
10.	Does business continuity and disaster recovery readiness have support of top management in your organization?			

The following *Scorecard* is designed to measure your computer systems and readiness to handle a serious unexpected shutdown. This scorecard examines computer practices within your business, including backup, recovery, and archiving procedures.

#	Computer Management Scorecard	Yes	No	?
	Back-up and Recovery Best Practices			
1.	Do you backup your data regularly and include every server and hard disk?			
2.	Does your current backup and recovery methodology meet management's business uptime needs?			
3.	Do you always use the "verify" option to ensure your backups are working?			
4.	Do you use backup rotations to provide a good depth of file versions?			
5.	Do you know how fast your data is growing?			
6.	Have you selected a scalable backward- and forward-compatible solution (hardware and software) that supports data growth?			
7.	Are backups fully automated for unattended operation (autoloaders, etc.)? If manual, do you have a bulletproof process and follow written procedures?			

#	Computer Management Scorecard	Yes	No	?
	Archive Best Practices			
1.	Do you regularly send your backup copy to a safe, off-site archive?			
2.	Do you retain archive data for legally required duration?			
3.	Is media properly cared for when shipped, handled, stored, and used?			
4.	Is your archive system designed to facilitate data format standards and an archive tape tracking method?			
5.	Do you have a migration policy to "refresh" tape technology and data formats every three to five years to ensure truly permanent access?			
	Business Continuity for Disaster Recovery Best Practices			
1.	Is senior management fully committed to disaster recovery?			
2.	Have you conducted a business impact analysis to quantify and rank the financial risk of outages to all vital functions?			
3.	Have you taken action to mitigate known risks and single points of failure (e.g. power loss, physical access, etc.)?			
4.	Do you have a written BCP that includes backup and archive			

#	Computer Management Scorecard	Yes	No	?
	procedures?			
5.	Have you tested your plan using a worst-case scenario (loss of a facility)?			
6.	Did testing prove that you could meet all recovery time requirements?			
7.	Is your business continuity plan updated regularly to keep it current with business and staffing changes?			
8.	Do you have an adequate budget to support your disaster recovery program?			
9.	Have you standardized on industry-standard media, tape drives, software, and automated back-up solutions?			
10.	For 7x24 applications, do you remotely journal, log, mirror, or electronically vault data to your hot site?			
11.	Do you understand your disaster recovery costs, options, and disaster declaration procedures?			
12.	Do you bring multiple tape sets to a test or recovery with current, self-reliant documentation?			

What is *business impact analysis*? At a basic level it is a means of systematically assessing the potential impacts resulting from various events or incidents

Commonly, impacts resulting from other types of incidents (such as breach of confidentiality or loss of data integrity) are simultaneously explored, but this need not be the case when only considering business continuity planning or disaster recovery. However, there are certainly advantages to undertaking a comprehensive and wider focused exercise.

The Business Impact Analysis is intended to help understand the degree of potential loss (and other undesirable effects), which could occur. This will cover not just direct financial loss, but many other issues, such as loss of customer confidence, reputation damage, regulatory effects, and so on. The Business Impact Analysis covers:

- Financial impacts to the organization resulting from each business operation's inability to conduct operations for a prolonged period of time.
- Operational impacts relating to each business operation.
- Extraordinary expenses involved in continuing operations after a disruption.
- Current state of preparedness to resume business operations.
- Seasonal Impacts relating to each business operation.
- Technology requirements for resumption and recovery.
- Other special resumption and recovery resources.
- Information Systems support for resumption of time-sensitive operations.

The Business Impact Analysis is one of the most important steps in planning for unexpected shutdowns. The data gathered is pivotal to identifying key business issues and justifying the resources needed to mitigate business risks. The Business Impact Analysis determines the financial exposures and operational impacts resulting from a major disruption of services. It will provide your business with:

- The identity of its time-sensitive business operations and services.
- An analysis of the organization's financial exposures and operational impacts.
- The time frames in which time-sensitive operations, processes and functions must resume.
- An estimate of the resources necessary for successful resumption, recovery, and restoration.

In addition to a Business Impact Analysis, it is important to conduct a facility/structural vulnerability analysis. The Business Impact Analysis will provide the rationale and cost justification for risk mitigation and response, resumption, recovery and restoration-related decisions.

Review Initial Business Impact Analysis Results

Review initial Business Impact Analysis questionnaire data for completeness and consistency; request additional information as necessary. The initial review of returned survey data would allow the project manager to uncover any area of ambiguity in questions asked or answers given.

CONSULTANT Tips for Conducting Business Impact Analysis Interviews (all size businesses)

- Every major business operation should be evaluated using the Business Impact Analysis approach. Each line manager must be aware of the length of time that a particular service, business operation, or application system may not be available, and devise interim procedures to ensure the continuity of the most time-sensitive activities.

- The resumption sequences, potential time delays, or service postponements for each business operation must be documented and endorsed by senior management. Senior management may be called upon to refine business time-sensitivity definitions, adjust resumption priority sequences, or allocate additional resources and funding where resumption capacity becomes an issue.

- The business owner should use this information to support the business's strategies and any necessary investments in backup alternatives.

Identify Time-Sensitive Business Operation Processes and Application Systems

- Establish a method, such as business time-sensitivity ratings, of grouping business operations, processes, and application systems based on their importance to the overall function of the organization. Time-sensitivity ratings are usually expressed in terms of the minimum and maximum time that the organization can withstand an interruption of a particular business operation or application system.

- Record each business operation, process, function, or application system along with its time-sensitivity rating. A comprehensive Business Continuity Plan will document a single or multiple strategy and tasks for every level of business time-sensitivity.

The following table provides a simplified example of output from a Business Impact Analysis:

System or Business Process	Outage Duration	Business Impact	Financial Impact
Human Resources	Greater than 72 hours	Negative Employee relations	$2,000 per day
Order Processing	Greater than 6 hours	Unable to complete new orders	$15,000 per day
Customer Service	Greater than 4 hours	Unable to communicate outage to clients, lost service revenue	$25,000 per day

Chapter 3 Understanding the business: the Business Impact analysis

By John Glenn, CRP from his paper "Business Continuity Planning Made Simple – Almost"

The Harris Institute certifies John Glenn as a Business Continuity and Disaster Recovery planner.

He has been involved with creating Business Continuity Plans for Fortune 100s and government organizations since 1994.

Articles by the author have appeared in peer publications and in general media. His mirrored Web sites link to a number of Business Continuity articles and contain information for both the novice and advanced planner. The Web sites, subject to change at the whim of the site providers, are

- http://johnglenn.itgo.com/articles.html
- http://johnglenncrp.0catch.com/articles.html
- http://www.geocities.com/CapeCanaveral/8836/articles.html

Contact the author at JGlennCRP@yahoo.com or JGlennCRP@netscape.net.

Identifying risks

Risks to input

Input risks are risks that would prevent the business process from being completed. For example, if a process depends upon input via

- Email
- Faxes
- Snail mail
- Telephone calls

The planner needs to look at risks to each.

Using email as an example, the planner must consider:

- Desktop equipment
- Electricity (or the business function that manages power for the organization)
- Facility
- Internet
- Intranet (LAN)
- IT (as an organization)
- Telephone lines (or the business function that manages the telephone lines)

Try communicating via email sometime without a working mouse/pointer or with keyboard that is sending the wrong characters.

In other words, consider anything and everything that could interrupt email communication.

Risks from business tools

Play the "what happens if..." game. (This is Business Continuity 101.)

If the [name the equipment] fails, how can the business process be completed?

If [name a person or position] is unable to do his/her job, what is the impact on process completion? (This might be a good time to think about "succession planning," determining who will assume the leadership in the event a top manager is unable to fulfill the organizational responsibility.)

The best way to find out what tools are critical is to tour the work area. What is used? On the desktop, in the file cabinet, the copy room.

While you are at it, find out what the manager and the troops think would help them complete the process more efficiently and economically.

A Client manager once told me that Business Continuity really is "PROCESS RE-ENGINEERING." He was right. We look at processes to protect them, but at the same time we should be looking for ways to improve the process. The exercise is good for us, good for the folks working the process, and good for our Clients or Employers.

Risks to output

A risk to output is simply the reverse of a risk to input (**Risks to input**). What happens to the process when this business function is through with it? How is it handed off? To whom or what?

When does it stop?

How far does the Business Continuity planner have to go to consider the process "protected?"

As a general rule, the planner must go to at least the neighboring business functions or the vendors to assure that the function or vendor has a Business Continuity Plan to continue service for the process.

If you are an in-house planner creating an enterprise plan, you will know (sooner or later) what the neighbor business functions are doing to protect their processes (which in turn protect the current function's processes).

If you are creating a plan only for one business function, you will need to diplomatically find out how the neighbor functions protect their processes.

When it comes to vendors, you may need support from the Contract's people, but you, as the Business Continuity planner, have a valid reason to see each vendor's Business Continuity Plan.

When looking at vendor plans, make certain the plan is
(a) up-to-date,
(b) tested, and
(c) that there is a maintenance procedure in place.
THE Rule: No test = No plan; No maintenance = No plan

The ubiquitous "other" risk

Risks generally fall into three major categories:

1. Human
2. Natural events
3. Technology

Human risks

Human risks range from "human error" to someone "going postal." These are the hardest to avoid and sometimes the most expensive to mitigate. Consider the anti-terrorist activity at airports around the U.S. after the September 11, 2001 attack on New York's World Trade Center and Virginia's Pentagon. (Yes, the Pentagon is in Virginia, not Washington DC.)

Natural events

Natural events include flooding, the most common risk, and other weather and geological events. Many of these events can be predicted with fairly good accuracy; even tornados can be anticipated based on specific weather predictions, and mitigation measures are well known.

Technology risks

Technology risks run the gamut from a loose connection to a failed system. Technology risks usually can be avoided by redundancy, but that is an expensive option. It is far less expensive to perform preventive maintenance based on manufacturer's Mean Time Before (Between) Failure (MTBF) and Mean Time To Repair (MTTR).

That still doesn't prevent someone from tripping over a cable ... but is that a technology risk or a human risk?

What about terrorism?

For the most part, terrorist activities parallel accidents.

For the Business Continuity planner, it makes no difference if a plane *crashes* into a building or is *flown* into a building. The result is the same. If the building in which the process you need to protect is in a take off or landing pattern, aircraft accidents must be a very real concern.

During World War II a B-25 bomber flying in a heavy fog
crashed into the Empire State building. That was an accident

caused by weather, a very tall building, and probably an inexperienced flight crew or instrument failure.

If the building is near a railroad track, barge canal, or major truck route, you must consider a HAZMAT event. It could be a terrorist action, but more likely it would simply be an accident.

With the exception of terrorism-by-mail, ***most*** terrorist actions mimic accidents or human risk; plan for accidents and human risk and you are planning against terrorists.

Final thought: You cannot **absolutely** defend against terrorists.

Philosophy: Plan for the worst; hope for the best.

Risk assessment - rating the risks

Risks are rated by "probability" and by "impact to the business."

Probability

How likely is a risk to occur for a **business process**?

Some risks we can anticipate based upon history. We know, for example, that certain areas are prone to flooding. We know when flooding typically occurs. If our Client/Employer was foolish enough to build on the flood plain – and some are, I know – we know to load sandbags in the flood season.

We know that mechanical and electrical parts give out. Most "long-life" components have MTFB/MTTR ratings; when the equipment nears the end of the shortest MTBF-component, we know it is time for preventive maintenance of the equipment.

Some risks have a "high" probability in some locations or seasons, and "low" probabilities in other locations or seasons.

Probability is rated on a scale of 1 to 3 (or 1, 2, 3), equating to low (1), medium (2), and high (3).

Impact

What is the impact **on the business** if the risk occurs?

In order to measure the impact, the Business Continuity planner needs to know

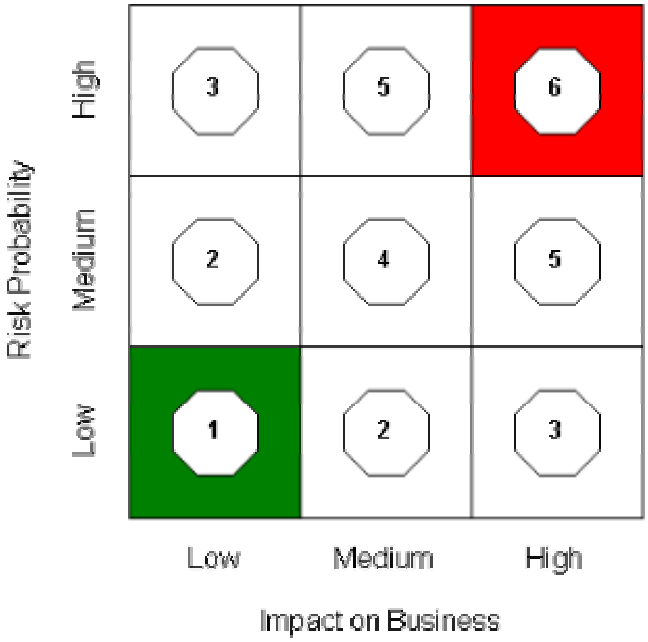
- How much income is lost for, typically, 1 hour, 1 day, 1 week, and 1 month
- How much it will cost (overtime, supplemental staffing, additional equipment) to "catch up" after an outage of 1 hour, day, week, and month
- What damage can be expected to be done to the organization's image
- What damage can be expected to be done to the organization's financial status (stocks, bond rating)
- What penalties will be applied by regulating agencies if the organization is unable to complete a critical process for 1 hour, day, week, month

The assumption is that full or nearly full operation will be restored within 30 days. The 30-day period may not see the entire operation functioning as it did before the disaster event – people may be working from temporary facilities – but the Level of Service will be (almost) Business As Usual.

Impact is rated on a scale of 1 to 3; low = 1, medium = 2, and high =3.

Tic-Tac-Toe

In order to prioritize the identified risks, a 9-square "tic-tac-toe" matrix is used.



The planner marks the Probability and Impact rating on the matrix. Assume a Risk Probability of 2 and an Impact of 5. Add the numbers for a score of 7 (2+5=7). Another risk may have a Risk Probability of 3 and an Impact rating of 1 for a total of 4 (3+1=4). Avoidance or mitigation measures would be applied to the "7" risk before the "4" risk.

Smart planners keep a coin handy to resolve equal-number risks.

Chapter 4 Food for Thought as You Prepare for Your Company's BIA

by Harlan Dolgin, CBCP

For anyone who has performed a BIA, you know that there are many choices to make in how it is structured. This article will give you some food for thought on decisions that may impact the results from your BIA. Every company will have to determine for itself what will work best for their situation.

One of the first decisions you will be faced with is determining the methodology to use. Will you hire consultants, use BIA software, use questionnaires, interviews, or both? The answers to all of these questions depend on what you want to get out of the project.

The goals of the project will guide you to the correct answers on the questions above. Do you want to perform a high-level BIA, or get as much detail as possible? Do you want to cross-reference every single application to the business units that use it, or just the critical applications?

The size of the company will also impact your goals. The larger the company is, the more difficult it will be to drill down to the finest detail. Other experts in the field have suggested taking no more than four months to complete your BIA. I agree with this, because a BIA is a snapshot of your corporation at one point in time. The longer the project goes on the more likely that the data will be out of date as soon as it is published.

Once the overall goals have been determined, I suggest that you define the reports that you will want to use in the final report. This may seem like an odd time to worry about this, but it will save you several very big headaches later on. After you've gathered your data, and you are getting ready to prepare your reports, you will invariably realize that you want to report on some additional information that you don't have, or that you don't have enough detail on. This will force you to backtrack to gather more data or abandon that portion of your report.

Is this project one which your company is going to tackle itself, or do you want to contract it out? If you hire an outsider to do it, make sure that you stay involved in every phase of the operation. If you do, you will learn a tremendous amount about your organization.

For one BIA I participated in, our company hired a consultant, but we made it very clear that we wanted to be assigned to tasks just as if we were employed by the consultant. This worked very well throughout the project. We all participated in the kickoff meetings. The consultant performed one-third of the interviews, and we performed two-thirds (after several training sessions). We prepared the detail spreadsheets while the consultant wrote the final report, which we then edited before submitting it to management. It was a true partnership, and we learned some invaluable insights into our company that we would have missed had we farmed out the entire project. As a side benefit, we also saved our company about half the cost consultants normally charge for a BIA.

Whether to use software or not is another issue. I feel that software at best can be a good beginning, but it should not be relied upon as the sole determinant of your BIA findings. We owned BIA software at the time of one of our BIAs, but we chose not to use it, and instead developed our own questionnaire. This allowed us to capture quantitative and non-quantitative information. In my opinion, this worked very effectively, although it was also very time consuming.

The software issue leads into another quandary, whether to rely solely on a questionnaire, perform personal interviews, or use a combination of both. This will be determined in part by the amount of resources available to collect your data.

Questionnaires definitely have their place in data collection, but I don't believe they should be used as the sole means to have a manager rate the criticality of their business functions. If resources are extremely limited, this may be a necessity, but I would try to avoid it if possible.

A good use of questionnaires is to gather data that involve lists of items (such as software applications, vendors, vital documents, or interdependencies among business units). Another purpose of the questionnaire is for items that may require research or some thought before answering. How many employees are required for a particular business function? How many during peak periods? How much revenue would be lost if the business function couldn't be performed?

These types of questions take a lot of forethought to answer correctly. We also asked the managers to rate the criticality of each business function, but only because we were going to follow up with discussions about this during the interview. A number of ratings were changed during the give and take of the interview process.

If information did not fall into these two categories, then we did not put it into the questionnaire. We saved everything else for the interview. During the interview itself, having the questionnaire answers in advance allowed us to focus in on the key areas that needed to be addressed. It streamlined the interview, saving time during each of the 100 plus interviews that were held. Combining methods in this fashion gave us more information than either a questionnaire or interview by itself ever could have.

Determining what should go into the BIA report is also critical to its success. As stated above, it is critical to decide what information is going to go into the report, so you must make sure to ask the right questions during the information gathering process. If you would like several types of questionnaires, feel free to e-mail me at dolginh@bcbsmo.com, and I would be happy to send them to you. Every company should judge the effectiveness of these forms for your organization.

One main objective of the BIA is to capture the number of employees utilized under normal and peak operating periods, and then determine how many employees (or desks, in a multiple shift environment) are needed within the Recovery Time Objectives (RTO) outlined by your company.

If you aren't familiar with the term, RTO means the timelines within which you need to recover your business functions. There are several ways to define the criticality of business units. There are usually three to five levels, broken into mission critical, near mission critical (sometimes called "necessary" or "essential") and non-essential. To make it simple, you can even number them Tier 1, 2 and 3 or A, B, and C. These labels will mean different things to every organization. Mission Critical could mean minutes for some organizations or it could mean a week for other organizations, depending on your company's tolerance for downtime.

It is also important to gather information on your company's tolerance for data loss. While RTO measures your tolerance for downtime following a disaster, Recovery Point Objective (RPO) measures how much data can be lost prior to the disaster.

A simple example should illustrate this point. If you backup your data nightly during the week, and you have a disaster event at 4:00 p.m. on Monday, you have lost one full day's worth of data plus any processing since Friday night's backup. Add to those two days that it would take you to recover at your hot site, and you've potentially lost a total of five days. If your critical business units feel they

can only be down for two days, then losing five days of productivity might be unacceptable to them. You can use the BIA process to make them understand that the true length of an outage due to a disaster is the amount of data lost (the RPO) plus the time it takes to bring your systems back to life following a disaster (RTO).

Following the BIA, your business units will now have a more realistic expectation of how they will be affected during a disaster. The importance of this cannot be stressed enough. A good partnership with the business units is essential to a successful BIA, and to the health of the DR program altogether. The definitions for RTO and RPO should not be driven by the IT organization, but by the business units themselves. They are in the best position to gage the tolerance in your industry for an outage. Generally, the only time this is discussed in any formal way is the BIA process. Otherwise, it is usually dictated by IT, who are making some very large assumptions that they know what the business units want, or there may not be a concrete policy on the subject. Either way, don't let it happen to YOUR organization. Keep your business units involved!

One of my objectives during a BIA is to understand how every piece of software relates to every business unit. If you have a large organization with hundreds of software programs, you may decide this is too tasking. If so, make sure you get at least the top five programs that impact each business unit. Applications should have a criticality rating separate from the business unit's rating, because you should not assume that every business unit needs every application it uses within the same timeframe.

A business unit that has a recovery window of 24 hours may only need its two main programs up and running within that time frame. It may not need three other programs until the end of the first week, which might give you time to procure equipment and build it yourself, rather than including it in a hot site agreement.

Vendors, vital records and other equipment should be treated the same way. They all need to be rated based upon how quickly the information or relationship needs to be reestablished.

Once all of these lists are created for each business unit, it will become self-evident which applications, vendors, etc. are most critical. Your plans can virtually write themselves. Well, it's not really that easy, but the plan-writing stage does become much easier when the BIA is performed in such detail, and if all the business units have participated and taken it seriously.

Determining what constitutes a mission critical business unit will also impact your final product. There will certainly be monetary concerns of how each business unit affects the bottom line of your company, but you should also consider each business unit on other levels, including customer service, regulatory, legal, and whether other departments are dependent on this unit, such as a printing department.

Imagine not being able to print out statements that generate revenue for a few weeks. Yet many companies may not consider their print shop worthy of having a mission critical rating. In banking, checks and deposits need to be processed within substantial time constraints. If they aren't, there could be fines and a very big public relations mess, where it could lose business. Customers' account balances would also be affected. Yet, the department does not generate measurable revenue. It is, however, mission critical.

In determining how many business units might be critical in your organization, there are no hard and fast rules. However, the 80/20 rule has seemed to prove itself out over several projects. Approximately twenty percent of your business units should fall into the highest criticality rating. It will be higher if you are in a highly time-sensitive field. These twenty percent of business units will

require eighty percent of your efforts, and deservedly so, since they are the heart of your organization.

If you haven't tried a BIA in your organization for some time (or ever), this should give you enough food for thought to point you in the direction you want to go. There will be other issues and decisions to make, to be sure, but you should be able to develop your own technique, incorporating some ideas from this article, and your own experience on what will be successful in your company.

Harlan Dolgin, CBCP, is a Business Continuity Analyst with Blue Cross and Blue Shield of Missouri. He is a non-practicing attorney who has been involved in IT since 1994.

Chapter 5 Getting Started In Healthcare Disaster Recovery
Now for Something Completely Different!

by Kathy Lee Patterson, ABCP

As a Business Continuity Planner ("BCP") or Disaster Recovery ("DR") expert, have you had the opportunity to perform a Business Impact Analysis ("BIA") for a healthcare provider? Well it doesn't take long to realize business is conducted in a far different manner. Hospitals have a culture all of their own. One obvious difference is that the healthcare provider is driven by the goal of preserving human life, with all other business and infrastructure needs a far second.

Shortly after beginning, you will notice the information services (IS) departments of many hospitals are usually ancillary groups, treated quite differently than clinical departments. Budgets can be far lower than needed to adequately support IS initiatives, leaving many systems on the verge of obsolescence. Additionally, clinical departments often operate autonomously, purchasing proprietary systems from vendors without IS knowledge or input, and subsequently expect IS to maintain the equipment after the vendor departs. Only within the past 5 years have clinicians come to realize the importance of their computer systems, applications, and email and how these systems aid in providing patient care.

The exciting fact is that HIPAA has started to "wake up" the healthcare community to the importance of disaster recovery.

Last year I was asked to develop a comprehensive IS-based DR Plan for a major teaching healthcare provider. I started out by conducting a Business Impact Analysis to demonstrate to the institution what impact a disaster would have to the care giving ability, finances, and community support. It didn't take long to realize that asking the typical BIA questions would not ascertain the true impact a disaster would have on these hospitals.

Large teaching institutions are inundated with all types of surveys concerning grants, research initiatives, pharmaceutical development, etc. When I introduced this project during a BIA Kickoff meeting to the healthcare community and announced that a "survey" was coming their way, the looks on their faces turned ashen and the murmur echoed "not another survey." I realized that I had to "sell" them on the idea of filling out this survey and one way to do this was to force the realization that we were attempting to help their departments and clinical practices by protecting their data and, ultimately, their patients' lives. Patient care is the utmost concern to the providers and aren't we glad that it is?

If you are initiating a BIA for a health system or hospital that you are not familiar with, I strongly recommend that you obtain assistance from a reliable representative within the institution to introduce and show you the territory. Each institution has their own nuances and the sooner you learn those qualities, the smoother your project will run. You will save a great deal of time. Many hospitals are set on campuses with numerous buildings and many of the same departments are divided amongst different buildings. You will also benefit from the guidance they can provide in developing the survey questions, keeping you from making any improper assumptions. Healthcare institutions are very complex in nature and asking defined questions as to how their departments run will give you better perspective when presenting the findings.

Generally, in conducting a BIA, one of the major objectives is to find out what the financial impact of a disaster would be to the institution. In a clinical environment, this becomes a little more complicated. In a large healthcare institution, clinical departments may not know how much income they actually generate. Insurance payments and government regulations muddy the waters even more. The clinical practices are very familiar with their budgets and the costs of their required resources, but routinely have a difficult time quantifying how the absence of their computer systems would affect their bottom line. A survey of the financial department reveals they may have the numbers, but not be able to accurately portray the impact an IS disaster would have on the ability to render patient care. If you concentrate on securing the qualitative data from the clinical departments and quantitative data from the financial departments, a great deal of confusion can be eliminated.

Patient management is the key phrase to understand. In most cases, a patient is rendered care by a great deal of departments during a typical hospital stay, such as laboratory, nursing, radiology, food service, housekeeping, etc. Inflow and outflow questions are extremely important to calculating impact. For example, when scheduling an interview with a food service department, I was advised that they are not very important because they didn't generate income and therefore didn't feel they needed to participate in the analysis. Even though Food Service doesn't directly charge for in-patient meals, by law, a hospital will not remain open very long if they cannot feed their in-patients. They are extremely reliant on their computer systems to compile the patient's food requirements for each meal. Their inflow comes from in-patient departments via the network and their computer applications, and their outflow is the food that sustains lives and allows the hospital to remain open.

Conducting detailed interviews is crucial after you have reviewed the completed surveys from every department. But be warned -- have your questions ready and be prepared. As soon as a clinician feels you are wasting his/her time and the questions are not relevant to him/her, you will immediately be shut down and the interview concluded. Most clinicians will work regardless of whether or not the computer systems are functioning. One out-patient surgical department explained during an interview, that if they suddenly lost their critical applications and computers, they (1) would not know who was coming in that day for an appointment, (2) would not have their charts ready when they got there, and (3) probably would not be able to bill them effectively, but they would still feel compelled to provide their patients with the best care possible anyway. While you will surely agree that this is admirable, exactly how would you gauge the impact of a loss of the computer systems?

Well, here are a few questions that helped me squeeze the information required for my analysis from them:

1. If your department renders patient care, how many patients does your department treat per day?

2. What is the average amount per patient that your department bills for these services? (This might be difficult to ascertain, but is possible. Be aware of duplicates, such as Admissions - doesn't actually produce revenue vs. Surgery - which directly derives revenue.)

3. Could you continue to render patient care without your computers or applications? How long could you provide consistent level of care without these applications (This will provide you with the Recovery Time Objective "RTO")?

4. What is your monthly (or yearly) budget? (This will help you break down daily impact plus impress upon them what is really at stake.)

5. If you had to switch to manual mode, would you be able to secure additional personnel with the proper expertise on an emergency basis? Estimate the cost of such personnel or overtime for existing personnel.

6. What applications are you most reliant upon and who controls those applications? (Get them to explain which applications are "frills" and which are "mandatory" in continuing patient care. You will be surprised by the answers. This will define your critical business processes.)

After extrapolating this customized information from your participants, you can add the typical BIA questions to your survey. Don't just assume that all departments are 24 x 7. Many supporting departments are only open for business from 7 a.m. to 7 p.m. or other hours.

As in any BCP/DR project, senior administrative support is essential. Make the survey participants aware at the onset that senior management wants their department to participate in this project. A signed statement of support from the CEO will get you farther faster.

If time does not permit you to survey all the departments that make up a health system (there could potentially be more than 100 separate departments), divide the departments in three categories: Clinical (renders patient care), supportive (to the clinical departments), and corporate. In doing this, you can make sure that you are getting equal amounts of responses from the three categories, keeping your data more accurate. If you have the benefit of using a survey software product as I did, the data collection process becomes far more accurate and efficient.

After you have compiled all of your data and are ready to present your report to senior management, it is important to remember who your audience is. You are working with health care providers, and to them, patient care is paramount. If you speak only in technical terms and financial impact, you could easily lose their attention and further plans for development could be refused. Take the time to explain what a hot site is and how it is used; they will greatly appreciate it. You have to cross the business barrier, speak in their language and to their emotions. Mention the amount of hours it would take before patient care is inhibited, how many hours before public confidence would be jeopardized and when staff productivity would begin to slip. A simple example is the Admissions department. When a hospital admits a patient, insurance carriers need detailed information for pre-certification purposes within a 24-hour window. If your computer systems are down for one week, you might be able to admit patients and render care, but run the risk of not getting paid for your services. When you put it into those terms, you are far more likely to get buy-in from administration.

The BIA was a great learning process for the entire healthcare community. Since most of the departments are focused primarily on patient care, they never took time to think about how they would function without their computer systems and applications for a long period of time. Many participants noted that they would give more attention to better work-around procedures, inflow and outflow procedures and necessary back-up procedures (which all tie into the new HIPAA regulations). Your training and awareness has now begun and your Disaster Recovery project is on its way. Hopefully, if guided appropriately, healthcare professionals will embrace the importance of disaster recovery incorporating BCP into their healthcare mission in the future.

Kathy Lee Patterson, ABCP, is a Healthcare Disaster Recovery Specialist for the Healthcare Solutions division of Affiliated Computer Services. ACS offers innovative and effective outsourcing solutions for clients worldwide. To learn more about ACS, visit www.acs-inc.com.

Chapter 6 A Guide to Business Risks (Anything that can go wrong will)

by Eric L. Beser, CBCP

An unexpected shutdown will occur at one time or another; it's just a matter of when. In order to cope with these shutdowns, it's important to prepare a plan of action should a shutdown occur. This section looks at major disruptive events and provides tips and techniques from the field. Preventing something before it happens, or taking steps to protect one's business is called a "Risk Mitigation" or in military terms, a "countermeasure." One cannot prevent natural disasters from occurring, nor can one fully expect to prevent a major terrorist incident, train wreck, or hardware failure. Most of the time, the probability of occurrence of these events is quite low.

It's all about averages. The probability that a terrorist will strike your building is about 99.9999 percent against that event occurring (unless you are a military target). However, the probability of other events, such as hardware failure of a computer, human error at the computer, or thunderstorm with lighting and tornado in the month of May, is quite high. Use the nail factory analogy from the previous section. If you drive on a parking lot full of nails, at some point in time you WILL get a flat tire. Your "countermeasure" is to take a spare, check it occasionally for health, and not worry about it. It's the same with business risks. You have to look at the probability of that risk occurring, rank order the risk by probability, then create the actions that you follow should the risk occur. By planning ahead, and by testing these plans, your business will survive the shutdown because the shutdown will no longer be "unexpected," but rather planned for and rehearsed.

From The Experts:

In the recent TV program, NOVA, the issue of "Why the Towers Fell" was addressed. In it, one survivor, from a floor above where the airliners hit, detailed how it came about that he survived. In his account, one fact struck me as paramount above all ... he had a plan and took the steps to follow that plan. Just as sure as you need a business continuity plan for your firm, you also need a personal disaster plan for yourself and your staff.

Wise folks have been known to say, "If you fail to plan, you plan to fail." Having a plan works for survivors. Without a plan, you just become another victim.

-- Lloyd Colston
Mayes County Emergency Management
Pryor, OK USA
http://www.geocities.com/mccem

Biological Hazards

While every business must monitor the quality of the air and water available in its facilities, for those businesses that handle biological and chemical agents, the matter is especially delicate. Imprudent handling of such substances - including unsafe disposal methods - pose obvious physical

dangers that could jeopardize both employees and the physical integrity of facilities. Beyond that, the cost of clean up and repair, as well as potential litigation, could be enough to close a business for any length of time.

In this time of heightened national security, businesses that handle volatile material have special reason to take precautions. High-profile businesses in particular run the risk of becoming targets for terrorist activity. Businesses may also be targeted for perceived political alliances or proximity to highly populated areas. While a leak or possible spill may be detected early enough to be contained, the sudden intrusion of external forces wishing to wreak havoc cannot be predicted. In such cases, the only defense is to prepare.

Countermeasures:

- Check with water providers to ensure proper filtration procedures are used.
- Have specialists inspect ventilation systems. Clean vents regularly.
- Monitor air periodically to classify and quantify hazardous substances.
- Keep a record of individuals with access to all hazardous materials.
- Ensure that regulations are followed for chemical storage, handling, and disposal.
- Provide proper protective equipment and shower stations where needed. Decontaminate materials properly.
- Clearly label all containers; compile a list of chemicals at site(s).
- Provide material safety data sheets (MSDS) to educate employees.
- Inquire into delivery service companies' security measures.
- Brainstorm with local and state agencies about terrorist attack preparedness.
- Ensure personnel are knowledgeable about biological and chemical weapons.
- Enact strict facility and peripheral security measures to safeguard against terrorism.
- Train employees in dealing with chemicals and hazardous substances and first aid.
- Inform employees of communication measures and evacuation routes from hazardous sites.
- Establish contacts at local fire and police departments and hospitals.

Blackouts

Few resources find more plentiful and diverse uses than electricity. The monthly bill is enough to remind us of that. Lights, heat, telephones, faxes, and computers are leaves on the same vine. And like any extensive network, a failure in one area can quickly affect many others. Old and defective hardware finally quitting, unintentional interference from nearby construction work, or a wire worn down by freeloading rodents is all it takes to bring productivity to a halt. Because so many things can cause an electrical failure, it is among the most frequent interruptions businesses face. It's one area of disaster planning in which the phrase "not if, but when" unquestionably applies. Understanding your electrical system and having a plan for when it fails are two of the best ways you can help your business.

Bad weather, as we all know, is often the first cause of power failure. The elements have moods for every season, and every season marches in a new armory of natural hazards. Spring brings electrical storms, while summer's intense heat can be too much for local power grids. Winter brings reprieve from those threats, but, of course, freezing rain and heavy snow present new problems. Every region of the world has its own weather patterns, and for areas which experience extreme heat

or cold, or lie in the paths of tropical storms, it is especially urgent to respond with a robust and trustworthy plan.

It can be difficult to predict how long an electrical failure will last. Particularly in the case of regional blackouts, technicians may be occupied with other people experiencing the same disruption. Furthermore, if many people are without power, emergency generators may be in short supply. The longer your business is suspended, the harder it may be to reassure customers of the stability of your operations.

Countermeasures:

- Establish a relationship with a generator supplier in the area.
- Ensure the supplier will be available to rent equipment 24 hours a day or on weekends, if necessary.
- Have a backup supplier. Make sure that its feeder is not from the same substation as the primary supplier.
- If there is a lengthy blackout, the generator may run out of gas. It is important to have an arrangement to obtain backup fuel.
- Arrange to have an electrician -- either independent or affiliated with the supplier -- present to tie the portable generator into the building.
- Check and maintain the main transformer for your building.
- Have an estimate of how much power would be needed in the event of a blackout.
- Store flashlights and batteries in a designated area.

Blizzards

In the realm of natural disasters, blizzards are certainly among the most ferocious. Bringing fierce winds, frigid temperatures, slick ice, and snow that accumulates in huge drifts, blizzards make their assault on many fronts. Winds bring down trees onto buildings and power lines, ice paralyzes mechanical components and interferes with transportation, and steadily rising snow blocks roadways and crushes structures with its ponderous weight. Even if your facilities are operational, employees may be unable to leave their homes. In the aftermath of the storm, a merciful rise in temperature can precipitate yet another hazard: flooding from all the melting snow.

Again, the weather patterns of your area will play a determining role. Areas most likely to suffer blizzards are the Mid-Atlantic Coast to New England, the Midwest, and, of course, Alaska. Businesses between the Rocky Mountains and the West Coast are also at higher risk. Naturally, the coldest months of the year - typically November through March - are those in which blizzards most commonly occur. Keep your ears open for winter storm warnings. If you hear one announced, it means that snowfall of more than six inches within 24 hours and winds at or above 35 mph have been recorded or are expected within 12 hours.

Expert Advice (from Contingencyplanning.com):

There are real implications for a business when a blizzard hits. Companies rely on their information systems to keep their business going; they rely on power. It is not uncommon to have a power outage during a blizzard because of ice or a utility equipment failure. Keep in mind that outages that occur during blizzards can also be prolonged because it is harder for utility providers to get around. Businesses need to be prepared to face the moment that their power goes out and the hours - or even days - that follow. In the short-term an uninterruptible power supply (UPS) can be used to protect data and help a company through a momentary outage. For a long-term outage businesses can look at a generator solution to keep their power going for hours or days. However, this can be costly.

When it starts getting cold or there are blizzard conditions, many businesses bring in space heaters and kick on their furnaces. This can reduce the power quality, which leads to brown outs. Look at a UPS to maintain a steady voltage. It is also a good idea to talk to your utility provider to find out how susceptible you are to a blizzard and when your power would be restored.

-- David Slotten
Tripp Lite
Chicago, IL

Countermeasures:

- Stock flashlights, first aid kits, and a battery-operated radio.
- Keep water and non-perishable food on hand.
- Buy an emergency heating source and appropriate fuel.
- Purchase uninterruptible power supplies and a generator.
- Make cellular phones and/or pagers available to key personnel.
- Have computer data backed up offsite.
- Evaluate alternate site options.
- Create a plan for telephone backup. If considering rerouting calls, determine how it would be done and where the calls would go.
- Decide which winter conditions will warrant early dismissals or closings, and develop employee notification procedures for these events.
- Find out how your community handles snow plowing and determine if it is necessary to contract for private services.

Business Relocation

Putting aside the fury of the elements, there are few things more disorienting than relocating. We tend to downplay the psychological effects of a place, the way our daily routine subtly incorporates minutia of our working environment. Picking up and moving to a new home can be very demanding. It takes some time to find our bearings, to ensure that all systems are functional in their new arrangements. Relocation, like any other aspect of business protection, requires planning. A mismanaged move can result in lost files, non-functional facilities, and employee confusion.

Nevertheless, sometimes relocation becomes necessary due to financial reasons or insufficient floor space. Any business can make the move, if equipped with a comprehensive plan.

Expert Advice (from Contingencyplanning.com):

It's a good idea to contact a mover as far in advance as possible. If your company has a specific moving date, you need to find moving resources that can accommodate it. The busiest moving season is the summer, so work far ahead if that's when your company plans to relocate.

Before choosing a mover, it's a good idea to get several estimates. Make sure you know precisely what you want the mover to do. Going with a reputable and well-known company that can offer references is also important.

Have the movers visit the offices. By letting them see exactly what has to be moved, they can make suggestions as to how many vans will be needed, how many workers should be used, etc. Prioritize the sequence of each individual office move. The company must carefully plan this. Label all boxes and equipment. It is also a good idea to lay out a floor plan to specify where items will go once they reach the new location.

Preplanning can help lessen stress and ease the transition. Share the relocation policy with employees. Let them know the company will arrange what services for them and what they will be personally responsible for.

-- Cliff Saxton
United Van Lines
Fenton, MO

Countermeasures:

- Provide new contact information to business associates.
- Inspect new facility. Ensure carpeting and painting are complete prior to move.
- Assess new geographic vulnerabilities.
- Create a floor plan, detailing placement of furniture and supplies. Designate an employee to supervise movers, using the floor plan as a guide.
- Make a checklist of materials to be shipped.
- Contact shipping and moving companies about services, pricing, and time specifications.
- Contact telephone service providers to make sure lines are installed and configured correctly.
- Call utility provider to designate new power specifications.
- Coordinate efforts between service providers and staff to have computer lines, programs, etc. installed at the new location.
- Order supplies in advance.
- Arrange for garbage pickups.
- If moving to another state or country, work with a relocation agency on employee housing.
- Designate a staff member as an employee contact to field questions.
- Notify business partners and service providers. Determine how the move will affect these relationships.
- Alert customers via advance telephone calls or mailings.
- Have mail forwarded.
- Determine if it is necessary to relocate records stored offsite.

Communications Dependency – The Weakest Link

The NTL telecom company looks to have been saved from Chapter 11 bankruptcy, but only at the final hour. For the business continuity managers whose company's communications infrastructure is reliant on NTL services, the last few months have been a worrying time. For others, the NTL case serves to illustrate just how dependent many businesses are on their telecom provider,

which is often a business's largest single point of failure. In this article Patrick Cowan explores the issues and proposes actions that business continuity managers can take.

Take a minute and write your answers down to the following questions:

- Do I really have the freedom to choose or the ability to control the way I communicate? (Emphasis on the REALLY)
- Do I understand who ultimately controls all the information that I receive or give?
- Is the communications venue safe, privileged, reliable, redundant, and diverse?
- Do you realize that all your financial, health, and private information is traveling over vulnerable communications links?

In most Western countries, telecommunication services have been denationalized and instead of one state telecom operator, there are numerous competing companies, many of which are global players. Competition is only as powerful as the money that fuels it and mergers and acquisitions are the order of the day. Economies of scale (large) are touted as the best way to give the consumer more services and easier access to information. However, this comes at a cost: business consumers have lost the ability to choose and affect change. In addition, given the state of the communications industry and the manner in which it has utilized its limited funds, do you want to put your company's future in the hands of the next bankruptcy filing?

Ok, you have answered the questions and the answers are not pretty. So, what can you do about your perceived lack of ability to control your communications environment? The answer is quite simple: invest in the future of your company by developing your own controls over communication.

Start with the tools already at your disposal:

- Perform a comprehensive risk analysis of your business units, focusing on communications (internal and external). Identify the potential revenue loss for each critical unit based on communications downtime. You may be surprised at the result - maybe not the dependency, but at least the monetary loss.
- Want some fun? Just formally require details of your communications vendor's BC/DR plan for ensuring continued operation of your specific telecom service and watch the panic set in! If you were not worried before about the safeguards, you probably will be now. It is essential that you ensure that external vendors (suppliers of communication service) provide you with a comprehensive BC/DR plan specific to the service being provided. Your company pays good money for the service; a BC/DR plan is part of the "guarantee." Once you have obtained a plan document don't forget to interpret the plans critically and evaluate them for single-points-of-failure, then feedback on any unmitigated critical risks, with requirements for the vendor to close the gap. The vendor will give you anything as long as you are willing to pay for it! At this stage, you are starting to gain some control, but you still have no control over the communications pipeline. You will probably find that your primary service provider is only a middleman to other providers; so, the plan you receive from your primary provider must also include vendors that they depend upon.

If the above challenge is tough, here is an even tougher one, which will take diligent analysis! What you really need is a cost effective, long-term solution to communications dependency. The vendors you currently use go to the manufacturer and purchase the equipment that moves your traffic. What is stopping you from doing the same thing? The answer is nothing! I know, you are not a communications company. You don't have to be. The manufacturer will consult with you on your needs and develop a strategy with you. The manufacturer may prefer to do this to time given the reduced market for cutting-edge technology now being experienced. Who knows, this partnership with the manufacturer may pave the way for advancing communications methods beyond the middleman's reach. After you have started on the road to developing your internal network, you can then do a Request-For-Proposal (RFP) to communications providers to manage the network. In this way you control it, can hire and fire, and can get cost benefits from competition at will. Or, you may want to manage the process from "cradle-to-grave" yourself (there are considerable resources in qualified individuals available today due to company failures and layoffs). What about the connection to the central office, the fiber (the in-ground or aerial asset) you need to communicate with the outside world? You can in many cases purchase and develop your own local "back-bone" directly to your own equipment, collocated in the central office of your carrier of choice. Yes, this solution has a monetary cost to it, as does developing an internally controlled switch able diversity to another central office.

Bringing control of communications in-house is not for everyone. However, for companies requiring 100 percent uptime and redundancy married to diversity in communications, it is the only way to safeguard the information entering and leaving your company. It may be that after performing your analysis you cannot justify the expense at this time. That is a quantifiable risk that you can plan for. On the flip-side, prudence in planning for communications resiliency would, at a minimum, dictate you at least require a comprehensive BC/DR plan from your dependent vendors of choice.

Unfortunately there is no easy answer to your telecom dependency. Any solution you come to will require much hard work and probably much expense. However, if your company demands zero tolerance of downtime, you have no other option than to address the issue.

Patrick Cowan is director of corporate disaster recovery, Qwest Communications. He was previously manager of corporate disaster recovery for Director, Disaster Recovery

Qwest WWN 555 17th Street 9th Floor
Denver, Colorado
(303) 992-4134 Office
(720) 218-7668 Cell
1-877-710-3135 Pager
Pin# 8777103135

Civil Unrest

The forces of nature have already received due mention, but one should never underestimate the destructive potential of an agitated crowd. Whether it be the premeditated effort of an angry group, a public rally sliding towards chaos, or incidental street violence, the result is the same: damage to your property. Broken windows and defaced storefronts may be only the beginning, as the damage can penetrate inside. Fires may destroy equipment and eradicate essential files.

Businesses that send employees abroad or have satellite locations in foreign countries may be surprised to encounter civil unrest with greater frequency. Recently democratized countries, places with unstable governments, and particularly oil-rich countries where the likelihood of terrorism is

greater should arouse caution, particularly for American businesses. It is another case where a business's ability to plan ahead may determine its survival.

Expert Advice:

Those carrying out business abroad should read as much as possible about the countries to which they plan to travel. Information about a nation's history, culture, customs, and politics can be found in most libraries, bookstores, and tourist bureaus, as well as from travel agents and most international airlines. Foreign embassies or consulates in the United States can provide up-to-date information on their countries.

The U.S. Department of State publishes "Background Notes" on countries worldwide. These are brief, factual pamphlets with information on each country's culture, history, geography, economy, government, and current political situation. The Department also issues fact sheets, or "Consular Information Sheets," on every country in the world. The sheets contain information about crime and security conditions, areas of instability, and other details pertaining to travel in a particular country.

Source: The U.S. Department of State (www.state.gov)

Countermeasures:

- Prior to and during an anticipated strike or protest on or around your company's property, walk the perimeter of your facility and remove all items such as bricks or rocks that could be used as weapons, projectiles, or any other means of assault to personnel or property. Ensure that all trashcans, newspaper dispensers, dumpsters, and planters are fastened down.
- Establish a relationship with local law enforcement to determine resource allocation and whether crowd control measures, such as tear gas, are likely to be utilized. (Shut down fresh air intake valves for buildings in areas where deployment of these agents is likely.)
- Ensure that your corporate security department keeps your corporate facility's personnel apprised of police response measures well in advance of their deployment. This will provide adequate time for decision-making regarding how to best direct and protect employees and customers.
- Contact your company's landlord or property management company in advance of an anticipated event regarding properties your business occupies. Determine their level of planning for such an event.

In the Aftermath:

- In the event of violence carried out on an employee or employees in the heat of protest or other agitation of local residents, first attempt to move the injured or assaulted victims out of harm's way. Communicate to other employees in the area that a dangerous situation has presented itself and they must take appropriate precautions.
- Contact law enforcement (and emergency medical assistance and fire authorities, if needed) and inform them of what has occurred, the extent of damage and/or injuries, and your specific location.
- Implement emergency response steps as outlined in your business continuity plan. Ensure that appropriate management personnel are informed of the situation and that all critical functions and roles are covered.
- If the building has been damaged and appears unstable, evacuate employees to a safer area. After the threat of violence has passed, the company (or building owner) should arrange a thorough investigation by a licensed structural engineer to verify that the building is safe for reoccupancy.
- After a workplace assault occurs, employers should provide counseling to those who desire such intervention to reduce the short- and long-term emotional effects of the incident.

Computer Failure

Internet Security Systems (ISS) has released the Internet Risk Impact Summary (IRIS) report for the first quarter of 2002. Developed by the X-Force, Internet Security Systems' security research organization and core protection knowledge base, the report includes statistical data and trend analysis derived from over 350 network and server-based intrusion detection sensors monitoring major multinational networks around-the-clock on four continents.

Summary of IRIS findings:

Hybrid threats: hybrid threats continue to pose the most significant online risk. In the first quarter, Internet Security Systems monitored 7,665,000 hybrid related attacks. Hybrid threats, including Nimda, Code Red, and Code Blue, are especially dangerous because they combine viral payloads with multiple, automated attack scripts against common computer vulnerabilities. The Nimda worm continued to be an especially dominant, expensive, and enduring hybrid threat. The attack rate for Nimda was an average of 3,500 per hour. These rates of attack remain ongoing and consistent.

Denial of Service Attacks: before the introduction of the hybrid threat, Denial of Service (DoS) activity dominated attack statistics. While DoS numbers have not gone down, they have been eclipsed in total activity by hybrid threats. DoS attacks remain an important and dangerous threat.

Vulnerabilities: during the quarter, over 537 new vulnerabilities were uncovered and documented by the X-Force. Two major causes of concern were significant vulnerabilities in the PHP scripting language, most commonly used in Apache Web servers, and multiple vulnerabilities in SNMP v.1 (Simple Network Management Protocol), the most common management protocol on the Internet. The SNMP vulnerabilities represent the largest multi-vendor security flaw ever discovered to date.

Pre-attack reconnaissance: combined with hybrid threats, network pre-attack reconnaissance accounted for over 80 percent of detected attacks. Vulnerabilities associated with port 21 (file transfer protocol) and port 22 (ssh remote login protocol) were two of the most prevalent reconnaissance targets. Software vulnerabilities also remained high on the target list for automated and individual reconnaissance.

Internet Threat Outlook

The short- and long-term risk level for the Internet remains high, with hybrid threats continuing as the most dangerous form of attack or misuse. Organizations that have carefully assessed the effectiveness of their Internet risk countermeasures but have not improved network, server, and desktop protection since the beginning of last quarter have fallen behind the threat curve and may experience a security incident. This demonstrates the growing need for a proactive protection approach to detect, prevent, and respond to an ever-changing threat spectrum, as well as the need for strong security policies and procedures.

Internet risk will continue to increase with new discoveries of software vulnerabilities and exploits. While Internet Security Systems believes these vulnerabilities will begin to lessen in frequency with the software community's increased attention to security as part of the development process, this decrease will not occur immediately. Vulnerabilities are therefore expected to remain problematic for the foreseeable future.

Home users, small office users, and Internet Service Providers (ISPs) will continue to grow as risk points in the overall threat equation. The rise in computer power and high-speed Internet access

has introduced a user population not resourced or trained to properly administer or secure its computers. Hybrid threats count on unsecured home, remote, or mobile systems to help penetrate the corporate perimeter. Internet Security Systems predicts that until intrusion protection systems become standardized, personal computers will continue to be easily infected by hybrid threats without the knowledge of computer owners.

Real-Life Lesson:

Of the multitudes of companies doing business on the Internet, few have adequate security measures in place. Insufficient Internet security can do more than jeopardize a company's Web site; it can provide pathways for hacker's intent on gaining access to your servers, systems, and data.

One business that relies heavily on Internet advertising was the victim of a denial of service attack. These attacks flood sites with phony requests and messages and can grind regular services to a halt. This company did not even know it was under attack until the stoppage occurred. In fact, the company was unaware it was vulnerable to attack.

A vulnerability assessment found a number of flaws and recommended appropriate security patches as well as the installation of a continuous monitoring system to warn of attack early-on. A typical analysis will find from 11 to 16 vulnerabilities per machine. Of that number, 50 percent are considered high risk and could provide immediate route access to hackers.

A hacker had no trouble gaining access to another firm's proprietary information. The way the administrator had configured the server, anyone could gain access to the hard drive. This is often done as a timesaving measure, granting access to all rather than inputting a long list of names. But "all" doesn't just mean all employees; it means anyone on the Internet can connect.

-- Christopher Klaus
Internet Security Systems
Atlanta, GA

Computer Virus

As computers have become the primary tool in business operations, it has become increasingly necessary to protect these systems from potentially damaging viruses. It is of paramount importance to protect your company's information from infection that can come in the form of a virus or its close cousin, the worm. Like a virus, a worm is a damaging organism that has the ability to self-replicate, but unlike a virus, a worm does not need to live in another program and can spread through your system by itself. This makes it a nastier, more dangerous type of virus that can spread rapidly. While it is almost impossible to completely eliminate the threat posed by computer viruses, there are precautions that can be taken to lessen the risks.

Combating the threat of computer viruses is a task that entails both prevention and post-infection recovery. A virus can strike a network without warning, crippling business operations for a substantial amount of time; therefore, it is essential to have an antivirus program set up in your computer. Even when a well-publicized virus, such as the Melissa virus, is out there and you have prior knowledge about it, it can still sneak into your system. The most common way for a computer to become infected is through e-mail or by visiting a website that carries a virus. Reliable firewall protection is the best way to protect against these types of infections. Once your computer is infected, the most important thing to do is to isolate the virus and protect critical data. Compromising the security of your company by spreading confidential data is the worst-case scenario in situations involving viruses and worms.

Playing safe

by JOHN GLENN, CRP, Certified Business Continuity Planner

While the effects of a computer virus or worm usually are limited to an "inconvenience," it can be both a costly and embarrassing inconvenience. A List I monitor had a virus warning and a worm warning today that prompts this article. Both target Microsoft Outlook products. Suggesting that organizations dump Microsoft mail products for other options is not the answer since Microsoft is here to stay, at least into the foreseeable future. Since there is not going to be a mass migration to alternatives - and there are many good options - we need to look at ways to avoid virus infections and worm infestations.

The procedures are fairly simple.

Empty the Address Book

Since the Address Book in Outlook and its variations often are a virus's targets, keep the Address Book empty. But where can addresses be stored?

Either on a local drive or in a word processor, text editor, or spreadsheet files.

Moving from either is simply a matter of "copy-n-paste." What about distribution lists - names and addresses grouped together for mass mailings? Same thing - put the lists into a word processor, text editor, or spreadsheet file. And "copy-n-paste" when creating an email. Formatting email addresses is described later.

Empty Sent Items folder

Something new to me is a worm attack on Outlook's Sent Items folder. The worm, picked up from a visit to a risqué Web site, sends out enticing emails to every address it finds in the Sent Items mail folder and sets itself as Internet Explorer's home page. Now having a triple-X home page may not ruin your day, but having your valued contacts get a "hey honey" message that may have your address in it may be more than a little upsetting to all concerned.

The best way to avoid having anything in the Sent Items folder is to make certain "save copies of sent messages" in the Sent Items folder is "unchecked." This is simple enough in Outlook: go to Tools > Options > Email options and clear the box under the Message Handling heading.

That solution may not be reasonable in a "Cover Your Assets" environment.

There are two easy alternatives.

- Alternative 1: BCC your own email address or, better, BCC an external BCC address.
- Alternative 2: Send copies in the Sent mail folder, and then "drag" them out of the folder and into a folder on your local drive.

The only problem with Alternative 2 is that it may be necessary to rename the file; email utilities accommodate files with the same name; most operating systems do not. This is not a serious problem; simply append a two-digit number (00-99) to the email subject.

Moving email - incoming and outgoing - off the email server to the local drive makes good sense anyway. If a message is important enough to save, it is important enough to save on the local drive. Why? If the network fails, mail on the mail server may be inaccessible; if it needs to be referenced, you are out of luck. Setting up a main email folder with sub-folders is a no-brainer whether is on the email server or on the local drive. One other benefit of moving mail from the mail server is to keep the server administrator happy; they hate it when users clog "their" hardware with no-longer-needed files. Since you may need the SysAdmin to restore some lost files later in life, it pays to be nice to them now.

A few quick words about attachments and downloads: don't open attachments unless you asked for the attachment. In particular, never open an *.exe, *.scr, or *.vb (anything) unless you asked for the file; these files are notorious for carrying viruses. It's good practice to simply blow away unsolicited attachments. All corporate PCs should be blocked from installing any applications and utilities. If a program is needed - Adobe Acrobat Reader, for example - whoever maintains the systems should download the file and install it. If you are allowed to download files, bring down files only from known good sites (such as Adobe's).

Experimenting with addressing

There are two basic address forms: with and without the addressee's name. If you wanted to comment on this article, you could key JGlennCRP@yahoo.com into the email utility's TO field and that would be enough to get the message to me.

If you wanted to be fancy and add my name before JGlennCRP@yahoo.com you might, depending upon your email utility, need to put quotes around the name and angle brackets on either side of the email address: "John Glenn". Some email utilities (Netscape for one) automatically strip away unnecessary quotes. If you have non-alpha characters (, . - _ ;) in the name, e.g. John Glenn, CRP, you almost certainly will need to "quote" the name.

Most email utilities, Outlook included, allow commas as separators in address fields (e.g. "John Glenn, CRP", JGlennCRP@netscape.net). Outlook requires the user to tell it that commas are used as separators by (according to Outlook's on-line help):

1. On the Tools menu, click Options.
2. Click E-Mail Options, and then click Advanced E-Mail Options.
3. Under "when sending a message," select the "Allow comma as address separator" check box.

A semicolon still may be used to separate e-mail addresses. Determine what your email utility requires by sending a test email to several people who can quickly tell you if they got the message.

Message which prompted this effort

** Sophos has issued a warning about the JS/CoolSite-A JavaScript worm, which spreads by exploiting a security vulnerability detailed in Microsoft Security Bulletin MS00-075. According to Sophos the worm arrives in an e-mail with the subject: "Hi!!" and the body text: "Hi. I found cool site! http://[omitted] It's really cool!". If the link is*

followed, a malicious script code from the resultant web page is run which attempts to send the same message to every e-mail address on e-mails held in the Microsoft Outlook 'Sent' folder. The script also resets the home page of Internet Explorer to the URL of a specific pornographic web site.

Expert Advice (from Contingencyplanning.com):

Prevention is the first and most important step in protecting your business from viruses. Be aware that malicious viruses are out there, and make sure that your company has a good security policy regarding this threat. Make sure that you have an antivirus program set up on your computer and that it's functioning correctly. Ideally, you should check weekly to make sure your virus definitions are up to date. Another more obvious measure involves simply backing up your data to a different machine; this way, if your computer does become infected with a virus, you won't lose important information. It is also a good idea to change passwords in your company on a regular basis. If your computer becomes infected with a virus, the first thing that you should do is isolate it to that particular machine. Once there is virus in a computer, it is of paramount importance to make sure that it doesn't spread through the network to other users. After the infection is recognized, it is not that difficult to rid your computer of it. The real damage lies in what it can do before it is recognized. That's why the best way to combat viruses is smart planning and comprehensive protection software.

-- Vincent Weafer
Symantec AntiVirus Research Center

Countermeasures:

- Make sure that you have a license for all software applications installed on all of your computers.
- Acquire software only from reliable sources.
- Make sure that you have a good antivirus program set up on your computer.
- Consult technology-related news sources regularly to stay informed about the latest viruses and their characteristics.

Computer Hackers

LOS ANGELES, California (CNN) -- As Californians suffered under rolling blackouts last month, computer hackers were trying to breach the computer system at the California Independent System Operator (Cal-ISO), which oversees most of the state's power transmission grid, a spokeswoman told CNN.

Cal-ISO spokeswoman Lisa Szot said a Cal-ISO computer system in Sacramento was attacked for a brief period of time in late April and early May. Szot said the system wasn't altered or harmed in anyway, but hackers did attempt to do so.

June 9, 2001 Posted: 4:54 PM EDT (2054 GMT)
From CNN Website

Hacking can occur anywhere at anytime. No matter where you are or what you do, it is likely that you are dealing with a computer, whether directly or indirectly. Paying with a credit card, making reservations on an airplane, depositing money in your bank account, and even making a phone call all involve computers.

Part of the problem is a combination of naiveté and, consequently, vulnerability. Most businesses are unaware that hackers are able to access their secret files, much less tamper with them. The solution, therefore, is knowledge and computer security.

Countermeasures:

- Create a tough set of passwords.
- Create backup copies of all appropriate electronic documents.
- Research, evaluate, and select an off-site storage facility. Ask about storage methods, facility locations, security, access, climate control issues, and classification and labeling procedures.
- Keep track of employees that have authorized access to classified documents.
- Make it clear to all employees that desktop modems are not allowed and that all traffic must be via sanctioned equipment and systems.

Just-In-Time Delivery Malfunctions

Initially instituted in Japan, where the technique was developed, just-in-time delivery (JIT) has moved worldwide. More and more US manufacturers are using just-in-time delivery for their operations as a means to cut costs and streamline production.

The basic concept of JIT is to receive what is needed just in time for it to be used. This places the responsibility on the supplier to get what is needed to where it is needed, just before the time it is needed.

In JIT systems, the parts required for final assembly are pulled in small batches from the supplying work centers. Not having to store materials on site cuts manufacturer's costs, while ensuring that they have a reliable, familiar supplier that they can trust to provide them the materials needed for production.

In any sort of business where the company relies on a supply chain, whether it's manufacturing, retail, or the food industry, a contingency plan should be in place to deal with emergency needs. If there is a problem with production on the manufacturing or plant floor, there should be an immediate solution. The supplier that you choose should have a just-in-time delivery program that

will respond to your needs immediately. They should be available to your company during all operating hours.

As valuable as JIT has proven to be, it exposes manufacturers to a variety of possible business disruptions. A natural disaster could wipe out one or more of a manufacturer's suppliers, a strike at a supplier's location could occur, communication failure between manufacturer and supplier could go down, or even a labor dispute or shutdown at a courier service could spell trouble.

Regardless of the cause, a manufacturer missing a part on the plant floor must stop operations until it can be supplied. Therefore, a business that relies on JIT cannot be run at its optimum level without a developed contingency plan that addresses the relationship between a manufacturing floor and the supply chain.

A manufacturing company must be able to coordinate the plant floor with the supply chain, and the supply chain must be able to communicate quickly and efficiently with the plant floor. A manufacturer that can minimize the time spent coordinating these aspects of production, and at the same time get maximum productivity out of its capital investment, has a competitive edge.

Countermeasures:

- Conduct a business impact analysis to reveal your company's vulnerabilities.
- Establish a contingency plan to deal with any kind of interruption in supply requirements.
- Establish a relationship with a parts supplier in the area.
- Make sure the supplier will be available to provide equipment during all of your company's business hours.
- Make sure the supplier will accommodate you with just-in-time delivery.
- Have a backup supplier for the parts you need.

Natural Disasters (Earthquakes, Floods, Hurricanes & Tornadoes, dam safety, wildfires)

Courtesy of FEMA

Earthquakes

Earthquakes have long been feared as one of nature's most damaging hazards. Earthquakes continue to remind us that nature still can strike without warning and, after only a few seconds, leave casualties and damage in its wake. Therefore, it is important that each person and community take appropriate actions to protect lives and property. This web site gives many suggestions for individual and community actions and provides links to web sites and publications with additional information.

Although earthquakes cannot be prevented, current science and engineering provide tools that can be used to reduce their damage. Science can now identify, with considerable accuracy, where earthquakes are likely to occur and what forces they will generate. Engineering provides design and construction techniques so that buildings and other structures that can survive the tremendous forces of earthquakes.

FEMA's Earthquake Program has four basic goals directly related to the mitigation of hazards caused by earthquakes. They are to:

- Promote Understanding of Earthquakes and Their Effects
- Work to Better Identify Earthquake Risk
- Improve Earthquake-Resistant Design and Construction Techniques
- Encourage the use of Earthquake-Safe Policies and Planning Practices

Preparing for an earthquake

by JOHN GLENN, CRP, Certified Business Continuity Planner

A planner acquaintance was told that a severe earthquake was imminent in his area. What, he asked, would I do in his situation? This is a person who once casually emailed that his IT facility was in the path of a rocket battle, so I have the utmost respect for his survival skills. I rattled off the standard preparedness ("business continuity") actions – make certain to back up regularly and ship the backups out of the area, look for alternate sites while his site is restored, be prepared to surrender his equipment for humanitarian use (tracking displaced persons, resources, aid workers, etc.), and "hope for the best."

Then I started to think beyond my fellow planner's data center.

Shifting my thinking from "business continuity" to "emergency management," the first thing I realized was that emergency management is very much like business continuity, only on a grand scale.

An aside: I, for one, think New York City's Emergency Management proved its worth on September 11. Its headquarters destroyed, it moved to a secondary location and did just about everything right.

The earthquake threat facing my acquaintance is centered high in some very high mountains. But, I have come to believe earthquakes are earthquakes and what holds for one holds for another, "more or less." For example, one of the main concerns for my friend is transportation, as in "evacuate the injured and bring in aid workers." While his problem is not unique, it is unusual.

Transportation

Earthquakes usually take their toll on the transportation infrastructure - roads, railways, airports, and ship ports. Where my friend sits, the transportation infrastructure is minimal, sometimes nothing more than an animal path. In Southern California, lack of highways would be an inconvenience overcome by delivering resources from the Pacific or bringing them in via helicopter.

But, if you'll go back a few paragraphs, my friend's quake-to-be will be "centered high in the mountains," too high for the typical commercial helicopter. Military machines will be needed to haul loads to high-altitude bases. Even if there were airports for Short Take Off (and) Landing [STOL] aircraft, the likelihood of damage to the fields would be too great to make STOL craft a reliable option. Unlike California, his quake's center is completely land-locked; sea access is not an option. In the wintertime, many of the animal trails that serve as roads are snowed shut.

Translation: even if helicopters can deliver the goods, the goods can't be delivered. That is, they can't be delivered unless someone brings in snowmobiles with the other resources. Are they suitable? We have to ask someone else for that information. (Proof again that plans cannot be created in a vacuum.)

Cache please

Whether in Southern California or the high Himalayas, it makes good sense to cache emergency supplies in areas likely to be inaccessible. (The mutual problem is security.) The difference between one location and another is population movement. Southern California, while its population fluctuates, always has a core community. Other places have mobile populations, populations that follow the food supply (e.g. goats, reindeer, fish). When the population is static, caching supplies - medical, food, shelter amenities (cots, blankets, portable chemical toilets) - is relatively a "no brainer." The "California problem" is that each site must accommodate more than the surrounding population so that neighboring populations unable to get to their caches can survive elsewhere.

Two problems exist when populations migrate: caches must be established along known routes, and security typically is sacrificed (who can spare the manpower to station someone at each site?). In the high mountains, the problem is a combination of both California and migration populations. The mountain residents typically move with their livestock, but settle in semi-fixed communities for a season. In order to protect these people, caches must be established along the routes taken by the migrants, keeping in mind (a) that the earthquake can happen at any time and (b) the community's demographics (e.g. ages, diet).

Avoiding a "got'cha"

Authorities setting up food caches must keep in mind the population's dietary restrictions (if any) and language limitations. The U.S. dropped hundreds of food packets to the Afghans, all carefully packed with food that observant Muslims can eat, but labeled in English, a language most Afghans cannot understand!

Multiple helicopter landing areas need to be identified well before the event.

Finally, the people - in Southern California and in the high Himalayas - need to know what to do and where to go when the quake strikes. Educating the people may prove the hardest part of the pre-quake activities. In Southern California, this means a multi-ethnic effort; this may be easier in the Himalayas, but the sensitivities of the populations must be respected if any effort is to succeed.

This point brings up the next critical component:

Communication

Getting the word to the populations that need aid resources is relatively easy in Southern California; instructions can be broadcast from relatively distant locations on local frequencies (assuming frequency and power restrictions are waived). Anyone who ever listened to the late Wolfman Jack on XOXO - most of young America in the 1960s - knows the power of radio.

Television may be too "high tech" to be an effective emergency medium. Gone are the days when each television was equipped with "rabbit ears" or an outside antenna; today's viewer more often depends upon cable - which can be broken - or dish antennas - which can be turned to a useless angle.

In densely populated areas, standard radios should prove satisfactory. In remote, isolated areas, the standard signal may be insufficient. (This is where this planner turns to a communications Subject Matter Expert [SME]; my knowledge of commercial [AM, FM] radio is limited.)

Short wave (HF) frequencies travel great distances, but receiver antennas must be correctly positioned for maximum reception. While short wave travels long distances and may be the ideal wavelength to convey information into the hinterland, it normally is not suitable for air/ground communication. This usually is carried on low-power UHF transceivers. Unlike HF transceivers, UHF sets are more "user-friendly" and should be relatively easy to learn to use.

The problem with all radio equipment is power.

Electricity may be non-existent - even if there was power before the quake, the event might disrupt it. Batteries have a limited shelf life, and every reader knows how easy it is for an appliance to be accidentally turned on - when the power is needed, it is not there. The answer is to provide at least a limited number of solar-powered transceivers or, alternatively, solar battery chargers. (I prefer the former, as it has fewer parts to lose or break.)

No matter how efficient the communications tools, if the Emergency Management people fail to speak the listeners' language, all the effort is wasted ... remember the food package with English instructions dropped to Afghans who don't know English from Latin.

While there are other concerns, one major one my friend may face that his counterpart in the US will not is an abundance of aid offers from foreign nations.

Help isn't always helpful

To our credit, when disaster strikes, we - humanity - usually put aside our political and religious differences to help our neighbors. About the only time the Greeks and Turks talk to each other is when they come to each other's aid after a disaster. The US never "officially" speaks to Cuba, yet some information travels between the two countries on an on-going basis. The problem is not an

inability to find nations to help the relief effort; rather, it is managing the various contingents. The Emergency Management operation must assign personnel to the most appropriate effort, and hope the volunteer is willing to take the assignment.

Since we usually have some warning that a quake (or storm) will strike, we can, and should, arrange relief efforts before the event. We should arrange who will do what; what nation will supply what resources. Having 500,000 tents for 50,000 people is about as beneficial as delivering Spam (R) to Israel - or Afghanistan, for that matter. Help must be coordinated; if it can be organized before the event, so much the better. In Emergency Management, the term is "mutual aid agreement." Beyond organizing the aid, the Emergency Management organization must keep track of the material from the time it arrives until it is put into the hands of those who need it.

It is an unfortunate fact that some aid is siphoned off by thieves and murderers; if the material can be closely tracked, the probability that it will reach the intended destination is increased.

IT still is critical

"I guess," my friend opined, "my IT operation isn't so important after all."

“Not true,” I replied.

It may not be needed in its current role, but it can be used for a number of humanitarian functions. Even if the operation his data center supports shuts down completely, the data center - if it can be kept operational - can be a major asset in getting aid to the people who need it.

Floods

Throughout history, people have settled next to waterways because of the advantages they offer in transportation, commerce, energy, water supply, soil fertility, and waste disposal. In spite of these benefits, however, our historic attraction to settling along rivers and streams is not without its drawbacks. Floods have caused a greater loss of life and property, and have disrupted more families and communities in the United States than all other natural hazards combined. The United States, as it moves into the 21st Century, is at a crossroads in the use of its floodplains. The nation may choose to use these flood-prone lands for the primary purpose of economic development, or it may take action to better balance their economic and environmental outputs.

Floodplain management is defined as a decision-making process that aims to achieve the wise use of the Nation's floodplains. Floodplain management aims to achieve a reduction in the loss of life, disruption, and damage caused by floods; and also tries to preserve and restore the natural resources and functions of flood plains (which, in turn, lessen damage potential). To achieve the goals of floodplain management, the nation must adopt a new approach -- one that takes full advantage of all methods available to reduce vulnerabilities to damages and, in parallel, to protect and enhance the natural resources and functions of the floodplain. This approach would achieve floodplain management through:

- Avoiding the risks of the floodplain,
- Minimizing the impacts of those risks when they cannot be avoided,
- Mitigating the impacts of damages when they occur, and

- Accomplishing the above in a manner that concurrently protects and enhances the natural environment.

The National Flood Insurance Program (NFIP) has played a critical role in fostering and accelerating the principles of floodplain management. Flood insurance is available to flood prone communities through the NFIP, which is administered by the Federal Emergency Management Agency. Prior to the NFIP, flood insurance was generally unavailable from the private sector and most states and communities did not regulate floodplain development. Dependence was instead placed on the construction of flood control projects such as levees, dams, and channels to reduce flood damage. Despite the expenditures of billions of dollars for these flood control projects, annual flood damages and disaster assistance costs were increasing at a rapid pace. In response to this worsening situation, Congress created the NFIP in 1968 to reduce flood losses and disaster relief cost by guiding future development away from flood hazard areas where practicable, requiring flood-resistant design and construction, and transferring costs of losses to floodplain occupants through flood insurance premiums.

The NFIP was broadened and modified by the Flood Disaster Protection Act of 1973, which requires the purchase of flood insurance as a condition for receiving any form of Federal or federally related financial assistance, such as mortgage loans from federally insured lending institutions. The NFIP has mapped floodplains in over 20,000 communities, and over 18,400 communities now participate in the program. Many states and communities have established floodplain management programs and adopted floodplain management statutes and regulations that go beyond NFIP requirements.

The National Flood Insurance Reform Act (NFIRA), signed into law in 1994, strengthened the NFIP by providing for mitigation insurance and establishing a grant program for state and community flood mitigation planning projects. The NFIRA also codified the Community Rating System (CRS), established objectives for CRS, and directed that credits may be given to communities that implement measures to protect natural and beneficial floodplain functions and manage the erosion hazard. The CRS is an incentive program whereby communities that exceed the minimum requirements of the NFIP secure reductions in the flood insurance premiums for their residents. Approximately 940 communities are currently participating in CRS. The policies in the CRS communities represent over 60 percent of all NFIP flood insurance policies currently in place.

Examples of flood mitigation include elevating homes and business above the base flood (a flood having a ?? percent chance of being equaled or exceeded in a given year), relocating homes out of the flood plain, and minimizing the vulnerability to flood damage through both structural and nonstructural means.

Hurricanes

One of the most dramatic, damaging, and potentially deadly events that occur in this country is a hurricane.

Hurricanes are products of the Tropical Ocean and atmosphere. Powered by heat form the sea, they are steered erratically by the easterly trade winds and the temperate westerly winds, as well as by their own energy. As they move ashore, they bring with them a storm surge of ocean water along the coastline, high winds, tornadoes, and both torrential rains and flooding.

Each year, on average, ten tropical storms develop over the Atlantic Ocean, Caribbean Sea, or Gulf of Mexico. About six of these will strengthen enough to become hurricanes. Many of these remain over the ocean with little or no impact on the continental United States. However, about five hurricanes strike the United States coastline every 3 years. Of these five, two will be major hurricanes measuring a category 3 or higher (defined as having winds above 111 miles per hour) on the Saffir-Simpson Scale. These storms can end up costing our nation millions, if not billions, of dollars in damages.

During a hurricane, homes, businesses, public buildings, and infrastructure may be damaged or destroyed by high winds and high waves. Debris can break windows and doors, allowing high winds and rain inside the home. Roads and bridges can be washed away by flash flooding, or can be blocked by debris. In extreme storms (such as Hurricane Andrew), the force of the wind alone can cause tremendous devastation, as trees and power lines topple and weak elements of homes and buildings fail. And these losses are not limited to the coastline -- they can extend hundreds of miles inland, under the right conditions.

Fortunately, a variety of measures can be taken -- both at the individual and community levels -- to reduce your vulnerability to hurricane hazards. Simple construction measures, such as the use of storm shutters over exposed glass, and the addition of hurricane straps to hold the roof of a structure to its walls and foundation, have proven highly effective in lowering damages when hurricanes strike. In addition, more complex mitigation measures can be pursued to further reduce a property's susceptibility. For example, coastal homes and businesses can be elevated to permit coastal storm surges to pass under living and working spaces.

Communities can further reduce their vulnerability to hurricanes through the adoption and enforcement of wind- and flood-resistant building codes. Sound land-use planning can also ensure that structures are not built in the highest hazard areas.

Tornadoes

Although tornadoes occur in many parts of the world, these destructive forces of nature are found most frequently in the United States, east of the Rocky Mountains during the spring and summer months. In an average year, 800 tornadoes are reported nationwide, resulting in 80 deaths and over 1,500 injuries. A tornado is defined as a violently rotating column of air extending from a thunderstorm to the ground. The most violent tornadoes are capable of tremendous destruction with wind speeds of 250 mph or more. Damage paths can be in excess of one mile wide and 50 miles long. Once, a tornado in Broken Bow, Oklahoma, carried a motel sign 30 miles and dropped it in Arkansas.

Examples of Mitigation Techniques

Hurricanes and tornadoes both have in common very high winds and the associated damage. After Hurricane Andrew, a team of experts examined homes that had failed and ones that had survived. They found four areas that should be checked for weakness - roof, windows, doors, and garage door. Some steps can be taken by most homeowners to reduce the vulnerability of homes to high winds. Others should only be done by an experienced builder.

Dam Safety

In this century, the rapid growth of the American economy and population caused a corresponding increase in the demand for water infrastructure projects. Legislation such as the Reclamation Act of 1902, the Tennessee Valley Authority Act of 1933, and the Flood Control Acts

of 1936 and 1938 resulted in large numbers of government-built new dams. Many of the new dams were larger in size because of advances in construction and materials, particularly in earth-moving equipment. Dam building in the United States peaked during the 30 years following World War II, when over one-half of the Nation's almost 80,000 dams were built.

In the event of a dam failure, the potential energy of the water stored behind even a small dam can cause loss of life and great property damage if people are downstream. Several dam failures in the 1970s caused the Nation to focus on inspecting and regulating these important structures.

In February 1972, a privately owned tailings dam in Buffalo Creek, West Virginia failed, devastating a 16-mile valley with 6,000 inhabitants. Because of the failure, 125 people were killed and 3,000 were left homeless. In 1976, Teton Dam in Idaho failed, causing $1 billion in property damage and leaving 11 dead. In May 1977, Laurel Run Dam in Pennsylvania failed, resulting in 43 lives lost. Six months later, Kelly Barnes Dam in Georgia failed, killing 39 people, most of them college students.

In response to the Buffalo Creek disaster, Congress enacted the National Dam Inspection Act (Public Law 92-367) in 1972, which authorized the United States Army Corps of Engineers to inventory and inspect all non-federal dams. The inventory was funded at that time; the inspection phase had to await the Kelly Barnes Dam failure, when President Carter directed the Corps of Engineers to inspect non-federal dams for the states. After the Teton Dam failure, President Carter issued a memorandum on April 23, 1977, directing a review of federal dam safety activities by an ad hoc panel of recognized experts.

In June 1979, the ad hoc interagency committee on dam safety issued its report, which contained the first guidelines for federal agency dam owners. In October of that same year, President Carter directed the federal agencies to implement the guidelines recommended in that report. The Federal Guidelines for Dam Safety encourage strict safety standards in the practices and procedures employed by federal agencies or required of dam owners regulated by federal agencies. They provide the most complete and authoritative statement available of the desired management practices for promoting dam safety and the welfare of the public.

Despite the strengthening of dam safety programs since the 1970s, dams continue to fail, causing fatalities and millions of dollars in property damage. In July 1994, Tropical Storm Alberto caused over 230 dam failures in Georgia, resulting in 3 deaths (ASDSO 1998 Survey Data). Between 1960 and 1997, there have been at least 23 dam failures causing at least 1 fatality. Some failures also caused downstream dams to fail. There were 318 deaths as a result of these failures (ASDSO 1998 Survey Data). The number of fatalities resulting from dam failures is highly influenced by the amount of warning provided to people exposed to dangerous flooding, and the number of people occupying the dam failure floodplain.

The creation of the National Dam Safety Program with FEMA as the lead agency is now 20 years old. Most dams in the United States are privately owned, located on private property, and not directly in the visual path of most Americans. These factors contribute to the challenge of raising the issue of dam safety in the public consciousness and getting the information on dam safety to those who need it.

Wildfires

The recent wildfires in the western States, the 1994 Tyee fire in Washington, the 1993 Southern California fire siege, and the 1991 Oakland Hills fires are examples of the growing fire threat which results from the Wildland/Urban Interface. The Wildland/Urban interface is defined as the area

where structures and other human development meet or intermingle with undeveloped wildland or vegetative fuels.

Wildland/Urban interface fire losses are not exclusively experienced in the west. Nearly every state has experienced wildland/urban interface fire losses, including the Pine Barrens in New Jersey, the Palmetto in Florida, and Jack Pine in the Lake States. Since 1985, approximately 9,000 homes have been lost to urban/wildland interface fires across the United States.

Individuals living within the wildland/urban interface can take steps to reduce the risk of fire losses. For example, you can create a Safety Zone around your home or business by doing the following:

- Stack firewood at least 100 feet away and uphill from your home.
- Clear combustible material within 20 feet.
- Mow grass regularly.
- Rake leaves, dead limbs and twigs. Clear all flammable vegetation.
- Remove leaves and rubbish from under structures.
- Thin a 15-foot space between tree crowns, and remove limbs within 15 feet of the ground.
- Remove vines from the walls of the home.
- Remove dead branches that extend over the roof.
- Prune tree branches and shrubs within 15 feet of a stovepipe or chimney outlet.
- Ask the power company to clear branches from power lines.

The risks of fire losses can also be reduced though use of flame retardant building materials on homes and businesses. For example, clay tile used on the roof can keep floating cinders from igniting the structure. Also, fire-retardant siding can be used to keep fires from quickly spreading.

The United States Fire Administration (USFA) serves as the national focus on reducing fire deaths, injuries, and property losses. In 1974, Congress passed the Federal Fire Prevention and Control Act, which established the USFA and the fire research program at the National Institute of Standards and Technology (NIST). The USFA works to involve the public and private sector to reduce losses through public education, arson detection and control, technology and research, fire data collection, and analysis and fire service training and education. NIST performs and supports research on all aspects of fire with the aim of providing scientific and technical knowledge applicable to the prevention and control of fires.

Weapons of "Mass Disruption"

By Evan Mendalson

The goal, or at least one of the goals, of most terrorist attacks is to create fear and hysteria. Perhaps this is why so many experts fear the deployment of a weapon of mass disruption, a weapon that prides itself on creating fear through mystery. Until recently, the phrase "weapon of mass disruption" referred to a massive cyber-terrorist attack on the nation's computer infrastructure. Now, however, scientists use the term to describe the "dirty bomb."

A dirty bomb, in laymen's terms, is a conventional explosive that has been packed with radioactive materials. The bomb first kills through the force of the explosion and then spreads radiation. However, as Richard Meserve, chairman of the Nuclear Regulatory Commission, said, the health consequences of a dirty bomb would be minimal and the greater concern is a "psycho-social one."

Meserve only reiterates what most experts say about the dirty bomb. For example, Steven E. Koonin, provost at the California Institute of Technology, said that the radiation from such a bomb would only lead to four additional cancer deaths among a population of 100,000. However, these same experts warn that most cities are not prepared to deal with the psychological and social ramifications of a weapon of mass disruption. As ABC.com reported, "Cities could expect to see hospitals overrun with thousands of fearful patients; businesses shut down for months, with billions in lost revenue; and increased levels of domestic and substance abuse as residents cope with stress." In other words, widespread panic would ensue.

Obviously, with all this talk of dirty bombs, the question becomes: how accessible are the radioactive materials to terrorists? Therein lies the problem. The likely ingredients in a dirty bomb – cesium, cobalt, and iridium isotopes – are widely used in industry and easy to come by. However, debate does exist over the ease with which terrorists could construct the bombs. Some people say that terrorists could easily construct the bombs, while others argue that they would kill themselves in the process.

Only a few countermeasures to the threat of weapons of mass disruption exist. One such solution is for businesses to educate their employees about dirty bombs, as education is the best defense against fear of the unknown. Clearly, any businesses that handle radioactive materials should keep close watch and inventory over these materials and alert proper officials of any missing chemicals. Lastly, as emphasized repeatedly in this handbook, businesses should have continuity plans in the event that they must evacuate their offices.

Transportation Disruptions

Travel is a mainstay among many businesses -- whether it's an employee's daily commute, sales call road trips, or conference travel. An unexpected break in the transportation process could create a ripple effect throughout an organization, causing key executives to be away from their projects longer than anticipated or stranding part of a team away from colleagues. Transportation is also part of the lifeblood of companies that provide or require shipping, mailing, and trucking services. If transport vehicles suffer a disruption, it could cause a catastrophic lull in the supply chain and a loss of revenue for businesses dependent on just-in-time inventory. Transportation disruptions such as traffic accidents, flight delays, and lack/loss of drivers occurring at any business could cause employee

stress, loss of work hours, reputation damage, and delay of receipt of packages and/or mail, as well as present the potential for human injury or death.

Whatever method of transportation you use for personal travel or for shipping materials, there is always the possibility that a disruption could occur. Part of the problem is unpredictability, as one can never tell when or where there might be traffic on the road or a delay in flight/train schedules. While certain methods of travel or transport may be chosen because they are quicker or safer, there is no method of transportation that is foolproof.

Real-Life Lesson:

We have a satellite tracking communication system in place for our trucks. The vehicles are equipped with keyboards so that the drivers can type messages to us and we can send messages to them. The satellite system can give us updates on our trucks every hour, giving us the ability to pinpoint their location by latitude and longitude. We can then figure out if the truck is going to be able to make its scheduled delivery on time. If the system detects that the vehicle is running behind, it will send an alert to our customer service department and to the truck's driver.

If one of our trucks is stuck in traffic, we will call the local police department to verify the traffic delay. Then we call the customer to let them know of the delay. If a vehicle breaks down, we find out if it's something we can fix, if we can transfer the freight, or if we could possibly tow the vehicle to the delivery site. We have had instances where we've had to tow the vehicle to the site because it was the only way to get the shipment to the customer. We want our customers to feel that we have their shipment covered.

In the end it all comes down to communication. We stress to our dispatchers not to work in isolation, to talk to their coworkers and others about what is going on. People give us their shipments because it is an emergency, or a "hot" shipment. It is important that we know what is going on with our shipments throughout the process.

-- Virginia Albanese
Roberts Express
(Arvada, CO

Countermeasures:

- Encourage key personnel to travel separately.
- Obey traffic regulations and speed limits.
- Conduct background checks on all company drivers.
- Look into providing driver safety-training courses for employees.
- Have all corporate vehicles inspected regularly.
- Plan for alternate workers to be used if drivers go on strike.
- Purchase tracking devices for all vehicles.
- Ensure all packages being shipped can be tracked by the service provider.

Chapter 7 The Changing Face Of Disaster Management

by Timothy Cousins

The management of the recovery effort after a disaster involves the intelligent anticipation of the consequences of immediate events as well as the control, organization and direction of future events. Rigid adherence to a plan is less successful than a more flexible, self-organizing, adaptive systems approach which is best facilitated by an informed external consultant who pairs with a relevant person within the organization.

Introduction

Collecting information about the recovery phase after a disaster is difficult given the sensitivity that companies feel about any disruption to their business. This paper gives an overview of the patterns and common characteristics of a recovery effort, which will be illustrated with examples from my experience.

In order to establish the relationship between planning and recovery I will include a brief reference to current planning practices. I will then discuss organizational adaptation after a disaster and the creation of predictive models; the stages of the recovery process and the crisis points; three group structures which emerge to manage the recovery including why one of these structures performs significantly better than the other two, and the meeting of stakeholders. Finally I will describe the role of the external Disaster Recovery Consultant in facilitating progress through the recovery.

Current Industry Practices

Because the field of disaster management is still relatively early in its development, it is not always clear what is meant by terms such as 'Business Continuity', 'Emergency Management' or 'Disaster Recovery'. An international cooperative effort to standardise a glossary of terms to correct this problem is currently underway, moderated by Steve Davis (2002). Meanwhile it is useful to make the following three simple distinctions: There is a before, a during, and an after.

> Business Continuity Planning, Disaster Recovery Planning and Risk Management are all concerned with a proactive approach to protecting an organisation from disruption by prevention, risk transfer or loss mitigation.
>
> Emergency management is concerned with the management of events as they unfold during an actual or impending situation that may cause injury, loss of life or destruction of property.

> Business Recovery Management is concerned with the recovery of a business after the emergency has receded and the organisation begins the process of rebuilding.

All three areas of current thought advocate a methodical approach to the development of formal 'pro-active' plans and follow similar lines:

1. Define objectives and assumptions
2. Gather facts and analyse requirements
3. Design the strategies
4. Create the plan
5. Implement the plan
6. Test the plan
7. Review/Update/Maintain the Plan
8. The execution stage (DRII).

(Australian National Audit Office, 2000; The Australian and New Zealand Standard, 4360:1999; The Disaster Recovery Institute International (DRII); The Business Continuity Institute (BCI); Safety Net, 2001; The UK Dept of Trade and Industry (DTI); Survive – The Business Continuity Group (BCG) and GlobalContinuity.Com).

It is recognised that the management of risk is an integral part of good management practice rather than a separate program. Optimally the planning process is considered to be ongoing and iterative in order to remain alive and current to the needs of the organisation. The allocation of resources, teams, tasks, recovery timelines and responsibilities is dealt with.

Though in general terms plans do not survive first contact with the reality of the aftermath of a disaster, it is my experience that organisations that have been through a planning process perform better after a crisis than those that have not, whether or not the plan has been activated. I attribute this to a function of the planning process rather than the plan itself.

Organisations that have not been through the planning experience take longer to get organised, find it more difficult to sort and evaluate information and to prioritise. Poorly formed perceptions of the loss are developed in the first few days after a disaster and these become difficult to shift. Confusion occurs when new information comes to light that does not correlate with the initial perceptions. There is difficulty relating the reactive strategy to the actual extent of damage and the workers are more likely to take extreme positions and operate in a hostile and avoidant mode. Vital opportunities to take control of the situation in the first few days are missed, and the recovery suffers.

Organizational Adaptation after a Disaster

The ability to change and re-organise to suit new conditions is the 'fitness' of the business in its environment. The pressure that demands changes is called the 'fitness landscape'. (Clippinger III. 1999).

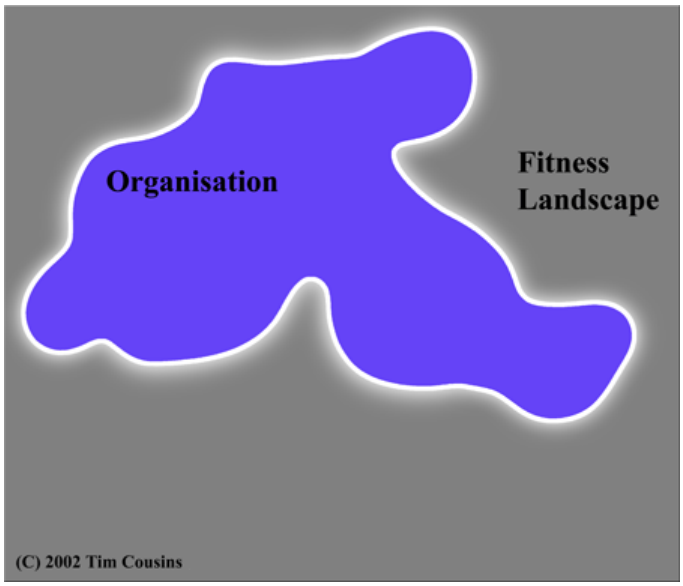


Figure 1 The Perfectly Adapted Organization

The organization has adapted perfectly to the demands of the fitness landscape.

When the fitness landscape changes, as in a disaster, so must the organization in order to survive.

Figure 2 A Changed Fitness Landscape

Changed conditions in the fitness landscape diminish the ability of the organization to function. It requires a corresponding organizational change.

Managers of the organisation must first correctly identify and characterise the altered landscape and then find and disseminate the right descriptions and definitions within the organisation to give

meaning and purpose to a responsive action. The most effective recoveries are realised when the participants are not directed from above but are allowed to develop their own responsive actions based on clear global objectives and well-developed understanding of the business requirements. For example, if the CEO gave a directive along the lines that the IT department will have the 'computer system up and operational by 2pm tomorrow at the latest' that then becomes the fitness landscape to which the IT department must adapt. On the face of it, complexity is reduced with the simple objective statement.

> *In 1994, I received instructions to have a computer system operational by a certain time after a fire destroyed the administration block of an electronics warehouse and repair centre. Alternative office space had already been secured and it was simply our job to relocate the server room and office computing facilities and establish a network link back to the warehouse. This was not a difficult task, and we easily met the deadline but the computers sat idly on the floor for another two days in the absence of suitable office furniture. Further delays involved the changed business procedures due to the distance between the warehouse and the office facilities.*

A little more time taken to develop a three dimensional views of the fitness landscape in the minds of all involved would have avoided these delays. We could have had greater cross-departmental cooperation, enhanced problem solving and a faster recovery. In this instance, however, the recovery was directed from the vantage point of a single person's view of the landscape that of the CEO, with little consultation with the staff involved.

In order to correctly identify and characterise the altered landscape a manager must make sense of clues, raw data and other evidence that arrives in no particular order from many different sources. Some of these clues may be graphic and clear, others murky and ambiguous. The perspective from which these clues are understood and conveyed to the manager will give rise to a view of the change that is invariably unique to each person. This view is codified and internalised as a model, which the manager then uses to 'look ahead' and anticipate outcomes.

Figure 3 The Perception of the Change

The organization perceives these changes with some degree of inaccuracy.

Each person involved will have their own view of the situation and their own corresponding internal model. The ideas and solutions that each person puts forward are formed in response to anticipated outcomes based on their own internal model. These views will change and/or compete for dominance and the group, as a whole is unlikely to arrive at a coherent view of the presenting problem. The diversity of realities can cause confusions and conflict and may threaten to reduce an organization to a level of chaotic functioning.

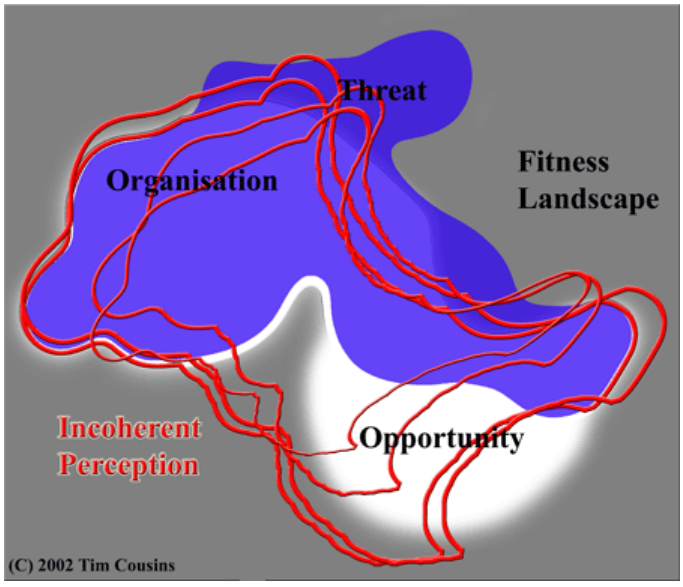


Figure 4 Personal Differences

People have different views. There is no coherent perception of the change or what is required.

It is important to understand who holds the guiding mental maps, how they are shaped and reshaped in response to the changing situation and how this is shared with others.

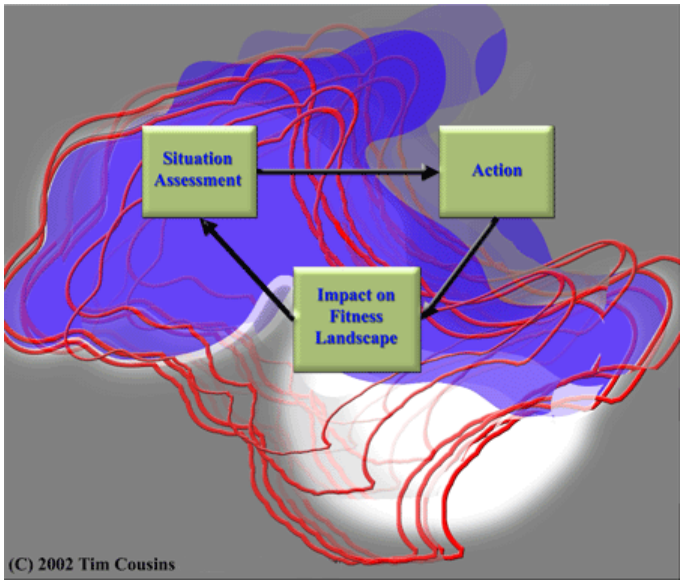


Figure 5 Constant Flux

The situation is in constant flux.

To complicate matters, the situation is in constant flux and those involved require fresh updates to their internal models. The greater the flux the more frequently the updates will be required. This update, if not forthcoming from the management team, will be found from whatever source is available.

The Post Disaster Crisis Timeline

Several important milestones occur during a recovery effort. These milestones represent opportunities for the whole group to collectively take its bearings in the changed and changing landscape. At each milestone there is an opportunity to influence the course of the recovery. It is usually at one of these milestones, when the recovery process is threatening to falter, that I am appointed to assist.

These 'Update' Milestones occur at:

- 4pm the day after the disaster

- "Shock of Awareness"

- At week one
  - "First Stakeholders Meeting"

- Friday before the third weekend
  - "Overwork or Family Subsidy." High expressed emotion and distress amongst family members.

- **At six weeks – MAJOR CRISIS POINT**
  - "Plan Not Working" Crisis

    - Shock of awareness

    - Second stakeholders meeting

    - Family Subsidy

- At three months
  - "Not nearly as good as it should be" Crisis

    - Shock of awareness

    - Second stakeholders meeting

    - Family Subsidy

A major crisis is precipitated at six weeks if there is no clear direction or map for the future or if the recovery appears to be going nowhere. It is my experience those six weeks seems to be about the length of time most people can tolerate uncertainty and ambiguity without some form of structure. It is often at this time that a political 'scandal' emerges and 'heads start to roll'. Both consciously and unconsciously, a round of finger pointing is embarked upon and major recovery strategies abandoned or modified significantly.

The Inventory Process

> Stanley Cohen describes in Folk Devils & Moral Panics, 1972, the Inventory phase immediately after the impact of the disaster as a phase "*during which those exposed to the disaster begin to form a preliminary picture of what has happened and of their own condition.*"

After life and limb are secure, the most significant and overwhelming need immediately after a loss or disaster is to remove, reduce or eliminate uncertainty and ambiguity. The natural response is to form a preliminary view, to seek out and 'take stock of' or 'inventory' the situation in order to understand what it is that has happened, to clarify ambiguous clues as well as to assess one's own personal situation and what it means for the future.

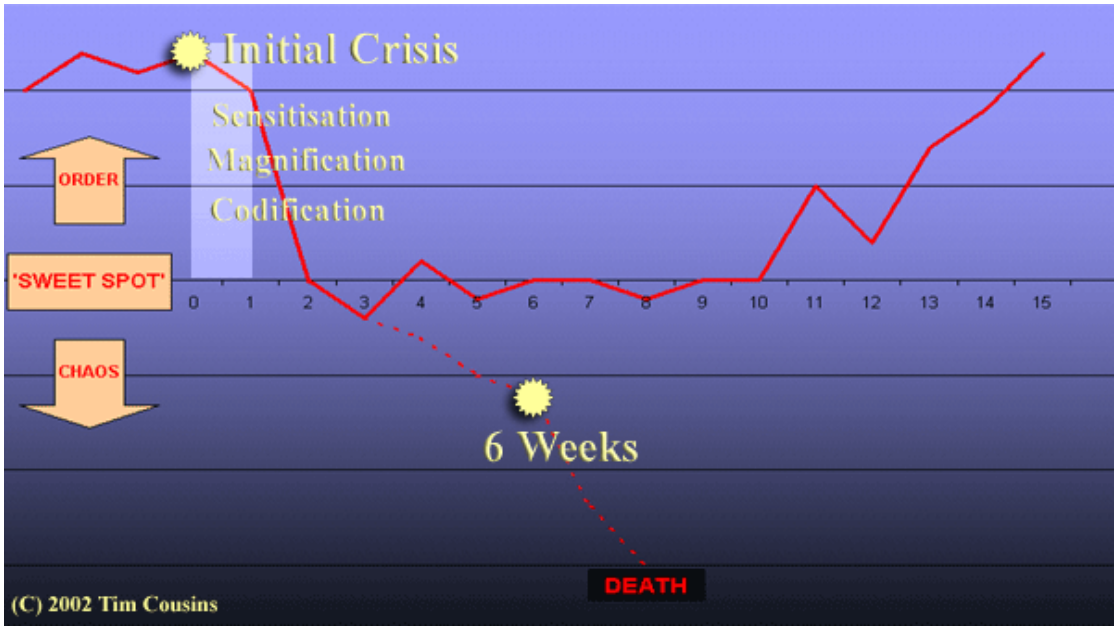


Figure 6 The Inventory Process

The Inventory phase is where those exposed to the disaster begin to form a preliminary picture of what has happened and of their own condition.

This inventory process is driven by the need for certainty and involves the collection and sorting of information from all quarters. Some of this information is based in fact, with clear supporting empirical evidence, but the majority of it, initially at least, is not. It is driven in part by the levels of anxiety experienced at the time and includes, often very uncritically, myths and gossip, which in turn are subject to further modification. As information of varying ambiguity and quality flows in about what has happened, opinions are formed and divergent views about the nature and extent of the losses, and perceptions of the magnitude and form of future risks emerge. As these divergent perceptions compete for dominance, three conscious or unconscious manipulations of the presenting evidence occur as part of the common inventory and 'weighing-up' of the evidence.

Cohen uses the terms sensitization and exaggeration in the inventory phase to describe processes that occur in community responses to moral threat. I have developed these for the inventory phase for the business situation and describe the processes of sensitization, magnification and codification.

a.) **Sensitization** is the name given to the hyper vigilance where proponents of one or other view become increasingly sensitive to evidence that supports their own or emerging view. It is a common experience for individuals to report faults and/or damage occurring after an event when the objective evidence suggests that these had pre-existed for some time before, but were simply not noticed, merely being brought to light with the heightened awareness and increased attention and scrutiny following the event.

b.) **Magnification** refers to the amplification of the (usually negative) consequences of the evidence that has now been noticed. The minor fault now becomes impossible to live with - or is an indicator of an incipient collapse. The 'stain' becomes a 'burn mark' and 'dust' becomes 'contamination'. Consider a situation where a perception is that the loss is all too much and overwhelming. A minor inconvenience that went more or less unnoticed before is now noticed and becomes 'the last straw' and further evidence of the dreadful circumstances that people find themselves in. If this view becomes the dominant view then the recovery effort will be seriously undermined.

c.) **Codification** is the process whereby a common understanding is reached about what has happened. The complexity and bulk of the information has to be reduced to manageable proportions. Making sense is a complicated affair, and involves a degree of anxiety that serves to cloud objective judgment. Each participant will hold a different view, and each will give the situation a different meaning as far as their own personal future or their perception of the group's future is concerned. All of the hard evidence, intangibles, rumors, personal perceptions, fears and expectations become bundled into easily communicated phrases, statements and 'media statements'. This is accomplished by reducing complex issues to simple 'language codes' or 'Tags' such as 'it is ruined' or 'it is OK' or 'it is not worth putting back into service'

The end result of this process is a coded narrative of the extent of damage that is fixed and over simplified, and may not have a great overlap with external reality. In the context of the dynamically changing fitness landscape, rigidity can be counterproductive.

The Structure of the recovery group

The way in which the different personal experiences and knowledge of the situation are given meaning and shared within the decision making group is heavily influenced by the informal communication structures that spontaneously emerge to process information and meaning.

The decision-making groups I work with fall into one of three structures or arrangements, which I have termed:

- Type 1. **Hostile Avoidant**
- Type 2. **Directed**
- Type 3. **Dialectic Pairing**

The defensive styles reflected in each of these classifications arise in response to the need to manage the underlying emotional threat of dissolution and chaos.

The structure of the Hostile Avoidant type and of the Directed type is driven along traditional hierarchical and historical patterns and workers often find it difficult to disregard the customary lines of responsibility and accountability. These groups are often shaped by the working style and emotional needs of bosses, rather than by the needs of the situation.

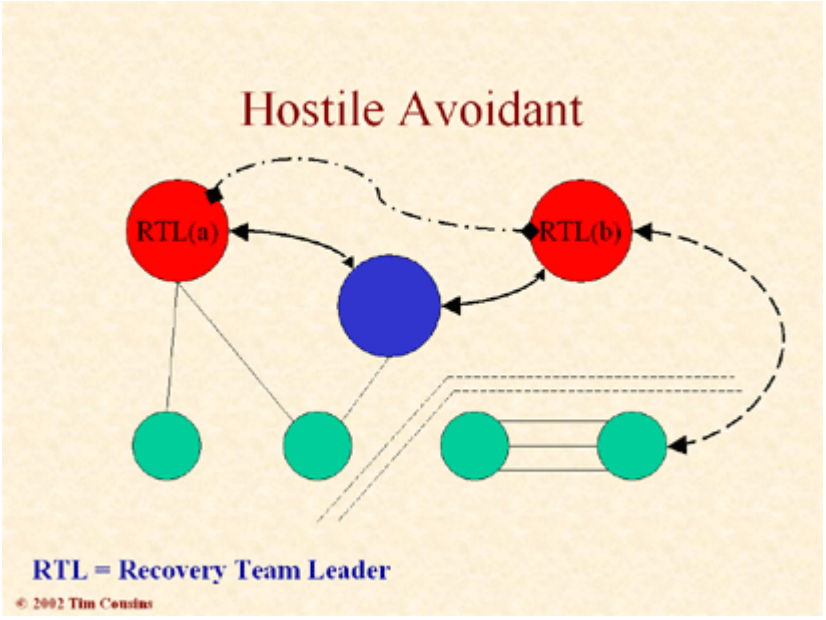


Figure 7 Hostile Avoidant

When a Hostile Avoidant structure prevails, communication and meaning is directed towards dominating or avoiding issues. The fundamental need for certainty remains unmet and the resultant anxiety is projected onto each other. The fighting with and/or avoidance of others ensure that any good ideas, offers of support and other positive aspects are lost in the tension of defensiveness. People caught in this structure follow procedure, but are anxious and generally unhappy. They contribute only a fraction of their true potential and this is reflected in the length and cost of the recovery.

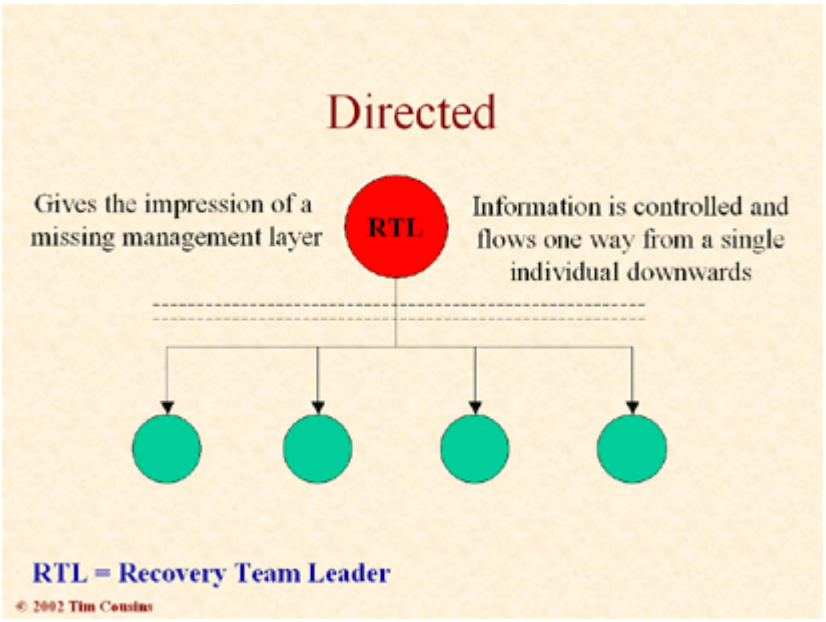


Figure 8 The Directed Type

The Directed group operates on the basis that there is a clearly identified and accepted leader usually mandated along historical lines of accountability. Where there is a pre-existing recovery plan, this may be adhered to slavishly. The leader supplies the subordinates' needs for certainty, security and nurture and in return, processes and assigns meaning to information for them. However in adopting this structure, creativity within the subordinate group is stifled. The threat of rejection and the implied denial of the supply of certainty and security ensure that only those suggestions and ideas in close alignment with the internal view of the 'gatekeeper' are presented. The net result is a narrow range of relatively homogenous options. The morale and strength of the response is highly dependant on the leader's emotional state and he/she quickly becomes overwhelmed with the amount and complexity of the work involved, with the inevitable flow on to the subordinates. Recovery situations where there is a tendency for this basic form to predominate are at high risk of running over budget and over time.

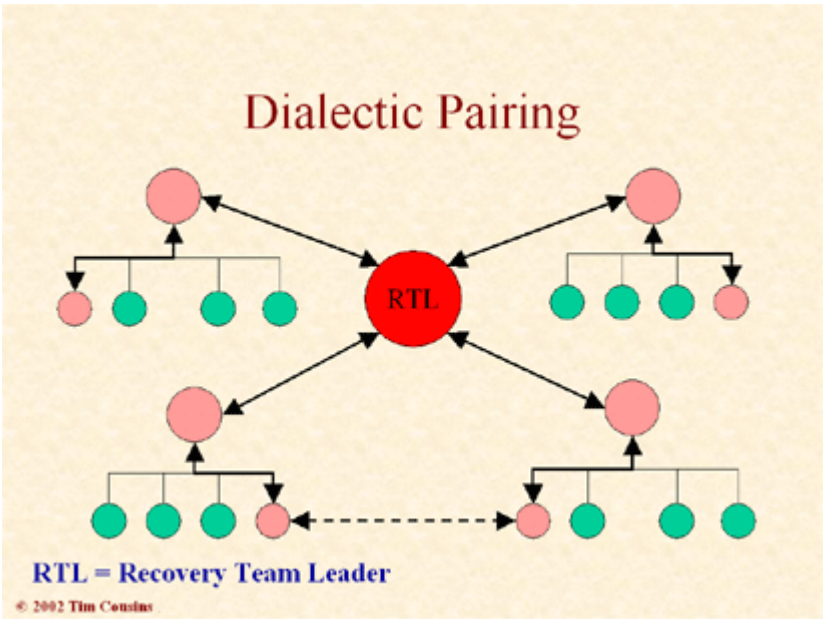


Figure 9 The Dialectic Pairing Type

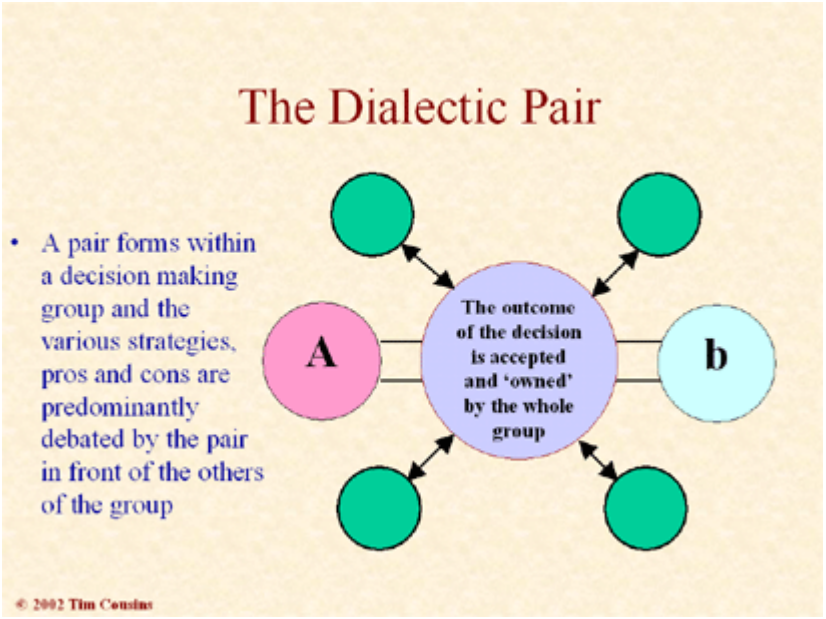


Figure 10 The Dialectic Pair

The Dialectic Pairing structure is the most successful across all the parameters of time, cost and work satisfaction.

In the aftermath of a disaster there is a great deal of information that needs to be rapidly and effectively processed, understood and relayed to others in the decision making team. The Dialectic Pairing structure is the most useful working unit for doing this task. It represents a dialectic functioning in which the whole decision-making group takes a part. A pair of group members who are able to discuss particular issues emerges within the group. The pairing is usually context sensitive

and will float between members according to the issues to be discussed, the expertise and informal authority of the members. One of the pair is accepted, formally or informally as a senior. It is the authority of the senior in the pair that breaks any deadlocks, but it is only exercised after a balanced discussion within the group. It is important that the pair demonstrate that any contribution, idea or view, however poorly formed is given permission to be expressed and is considered seriously. The various strategies and the pros and cons are debated predominantly by the pair in the presence of the others of the group. This discussion allows for the basis and complexity of the decision making to be observed, experienced and contributed to by the others, while at the same time eliminating the need for a second transfer and justification of the decision afterwards. In essence this process, by its very nature, builds a three dimensional view of the fitness landscape.

The recovery process, which operates in this structure, is characterised by high morale, creative and productive work, lowered anxieties and a sense of optimism for the future. Not only do these groups have a more dynamic and integrated structure, but they are also able to lift themselves beyond the threat of dissolution or chaotic collapse through a symbolic narrative of 'unity', 'the heroic effort' and other stories.

> *I was appointed to assist in a recovery of a company, which manufactured and distributed spectrophotometers and other hi-tech laboratory instrumentation. The venture was partially owned by an Australian bank in an unusual joint venture. There was a fire and the company, which was under-insured, was plunged into a dire financial position. The bank, as a partner, wished to shut the business down and liquidate rather than bother with an attempt at a recovery. Despite this added threat from the bank, the directors of the company were able to engender a symbolic 'heroic' response, which demonstrated such commitment of purpose and determination amongst the staff that the company was able to negotiate extensions of time and finally demonstrate financial viability. Despite the objective financial assessment having written them off after the fire, they are still operating and thriving 8 years later.*

When the Dialectic Pair structure does not occur spontaneously, it is often possible to assist a group to develop this mode of operating by integrating into the group as one half of a pair with a respected and significant member of the group. The person paired with is most helpfully a technical person or engineer.

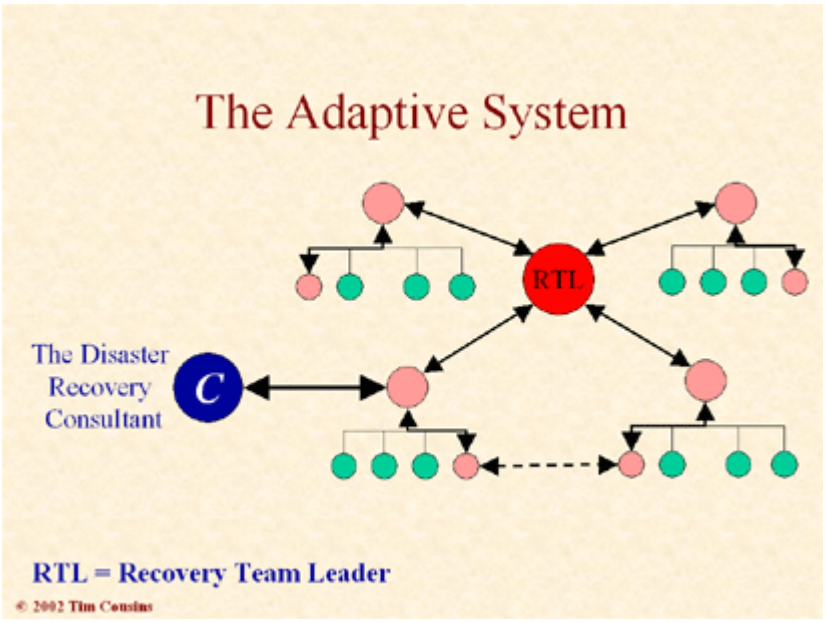


Figure 11 Forming the Adaptive System

Taking this concept a little further the pairing can be used to extend up, down and across organisational hierarchies and disciplines in a form of networking. It has tremendous power to control and manage the meaning and flow of information between those involved in the recovery effort. It is the flow of information and meaning in this manner that provides a substrate for group intelligence to emerge and with it the possibility of performing better.

Symbolic processes can inspire confidence, courage and commitment and prevent the group from descending into a Hostile Avoidant structure. Humor and play can be used to break down barriers and to reduce tension and encourage creativity. Personal stories of the disaster, of the close calls and the heroic efforts, as well as the myth of the 'rescuer' or the 'arrival of the cavalry' all make for a common binding narrative. The ritual of the early morning 'recovery meetings' held by the firm served, not only functional information and decision-making purposes, but provides a sense of identity and camaraderie for those involved.

The Stakeholders meeting

The 'First Meeting of Stakeholders' is held, usually at five to seven days post disaster. Representatives of Insurers, Brokers, Loss Adjusters, Bankers, Critical Equipment Manufacturers, Decontamination/Restoration Specialists, Technical Experts and others assemble in what is essentially a political meeting. The meeting is a necessary mechanism for understanding the political landscape through which the recovery needs to progress in order to address the differing interests of stakeholders. A process of sizing up occurs at this meeting, territories are mapped out, roles discussed, positions adopted and demonstrations of allegiance are encountered. Statements that

define strategic boundaries are made, such as "Under no circumstances will this course of action be taken. Regardless of the logic, it is just unacceptable" and "It is unsaleable."

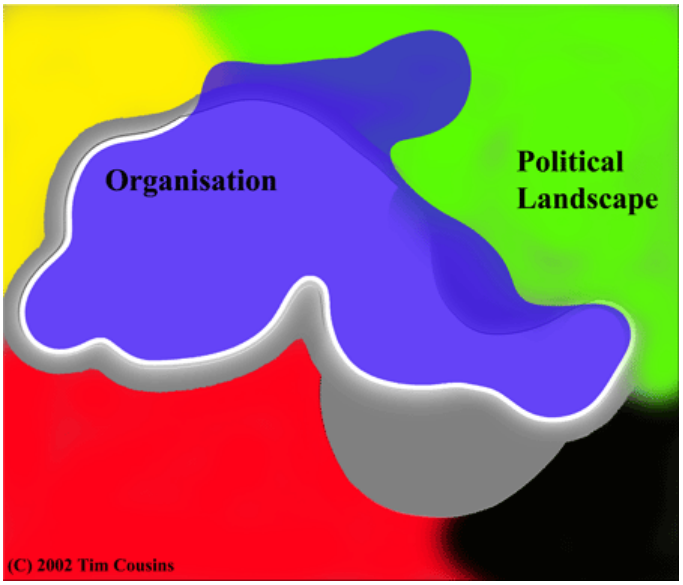


Figure 12 The Political Landscape

If the recovery progresses well, the stakeholders' meeting usually only occurs once in the life of the recovery effort. However, if the recovery is complicated or is progressing poorly at the six weeks stage, a political realignment becomes necessary. The realignment meeting of stakeholders at six weeks generates enormous interest, which is reflected in the large numbers who attend such meetings.

I was appointed to assist a recovery effort after a fire had destroyed and contaminated the majority of the electrical control equipment in the electrical services building of new power station that was nearing completion. I was appointed six weeks after the fire. My first task was to attend a meeting attended by representatives of the four consortium partners responsible for building the power station, the relevant State Government body overseeing the construction, The Lead Insurer, Loss Adjuster, and Insurance Brokers. There were twenty six people in all at the meeting.

The building of the power station was being funded by the State Government although ownership had not yet passed to them. It was intended that the State Government would then sell the operation to a third party as a going concern with a long term contract to supply power to the State. They needed to be certain that the rectification work was sound and could be shown to be the case to any potential buyer and therefore would not impact on the sale price.

The four consortium partners were bound by contract to honor the delivery date or be penalized by liquidated damages clause. The State Government needed the power station on-line for the anticipate seasonal peak demand which was in less than six months from the date of the meeting. The lead times on some equipment was too long to meet these deadlines and therefore had to decontaminated and repaired rather than replaced. The German manufacturers of the equipment were not prepared to maintain their warranty on any of the contaminated equipment and refused to consider decontamination or repair as an option.

There still had been no clear determination of the extent of damage and the recovery had stalled. There was intense argument about the way forward.

During the meeting it became apparent that the object of the meeting, though not publicly articulated, was to reduce or eliminate the influence of a specialist decontamination / restoration company. The prevailing political landscape was changed by the introduction and acceptance of me as an outsider. I was able to review the nature and extent of the damage to the power station, and begin to address the technical and political needs, thereby containing the anxiety of the group, and freeing up the process of creative problem solving. It took two days for me to integrate into the political landscape and a further week for the realignment to occur. The outcome of this process was that different arguments and objectives were able to be presented to the Insurers who held the purse strings. The recovery was ultimately very successful, but it could easily have been very different.

The Disaster Recovery Consultant

A pre-requisite for the consultant or manager navigating a recovery is the ability to integrate his/her own personal perceptions, reactions and anxieties so that a coherent internal model of the disaster situation and processes can be formed. This dynamic model can then be used to support and guide those involved in the recovery to become self organising, responsive and creative in their approach to problem solving.

An informed external consultant working with the organisation can get a better result than often can be achieved by internal efforts alone, particularly if he/she is appointed early. There is a need for containment of the situation both with respect to the emotions of the people involved as well as in relation to the damage to infrastructure, which may still be ongoing. When I am appointed early enough I have an opportunity to limit the initial confusion by holding and organising the flow of inputs and outputs long enough for some recognition, organisation and structuring to occur. This is where a contemporary holistic understanding of the shifting perceptions of reality, which constitute a crisis and its aftermath, gives significant advantage in the recovery process over any slavish adherence to a plan.

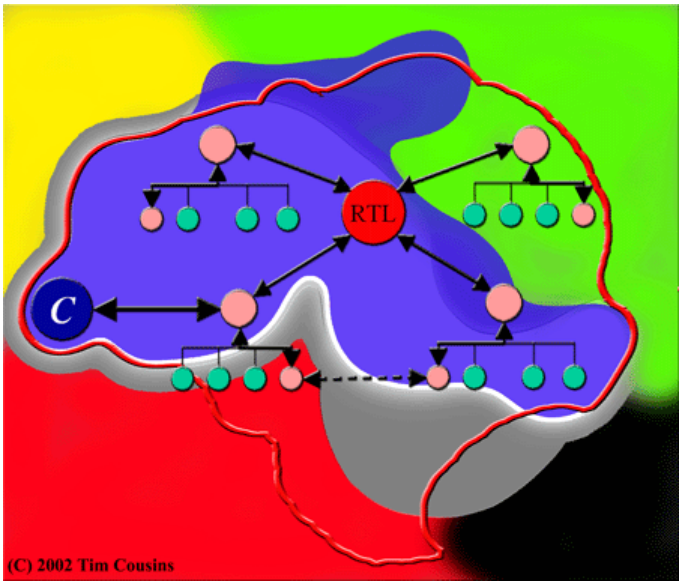


Figure 13 The Disaster Recovery Consultant

My first task on being appointed to a recovery is to assess the nature and extent of damage. A combination of technical skills and social skills becomes important as this assessment is done in the context and setting of a sense of urgency and high levels of anxiety amongst the people of the organisation. The different stories must be heard and a context provided for the experiences before creative energy and solutions to begin to emerge and develop in the decision making group.

> *I was involved in a situation where fifteen hectares of plant machinery in a carpet factory was submerged in five feet of water. I was called in after the water subsided and the first access was granted to the equipment. The quantity of machinery and size of the property was so large it took two and a half hours to complete the initial walk around. On arriving back to the central command point I found twenty foremen sitting around despondent, unable to initiate any action or to form any constructive plan.*

My first response was to have an informal public discussion about the normal physical operation of the plant. This discussion involved all of the staff present as they were drawn from all areas within the factory. It provided a new context, remote from the distress and despondency, and allowed a further series of general public questions about which machines concerned them the most. Then, after sharing some of my experience with electronics and corrosive processes, we were able to identify which machines needed attention first and within a very short time a constructive and practical action plan emerged. This plan involved placing orders for a short list of critical replacement parts and setting up a production line for stripping, washing, drying and protecting, circuit boards from ongoing corrosion.

Having defined the boundary of the immediate problem and communicated an understanding of the context of the damage, anxiety levels within the organization became dramatically reduced, and the

work of shaping the recovery began. As the recovery preceded, further group assessments of progress were made, boundaries were redrawn and action plans adjusted.

Regular update meetings both formal and informal became points of reference for the exchange of ideas and observations and for the sharing and updating of information from the field as well as for encouragement and support. Again, symbolic stories of 'The boat trip around the plant' and a 'Near drowning and subsequent rescue' served to lift spirits and unify the group

Despite the palpable unity of the foremen and the workers actually managing the physical clean up and recovery, there was a division and tension between them and the office staff. The office staff had clearly different priorities and sense of identity. The political friction that this difference generated, particularly over the allocation of scarce resources had to be managed. In this context, because I was perceived to be objective, technically and socially competent, without a conflict of interest and politically neutral, I was frequently sought out for an independent validation of various decisions and strategies and used as a sounding board for further possibilities. This use of me extended from the shop floor through management to the Loss Adjusters, as representative of the Insurer's interests.

Key Lessons Learned:

1. Participation in the planning process more important than the plan itself.

2. Resources allocation and availability

3. Integration of thoughts, perceptions and emotions

4. Combination of technical, social and political skills in the recovery manager

5. Recognition of Sensitization/Magnification/Codification issues

6. Knowledge and anticipation of crisis points in the recovery timeline.

7. Dialectic pairing

8. Consideration for family/social needs of recovery workers

9. Stories to bind

10. Find the 'sweet spot'

Conclusion

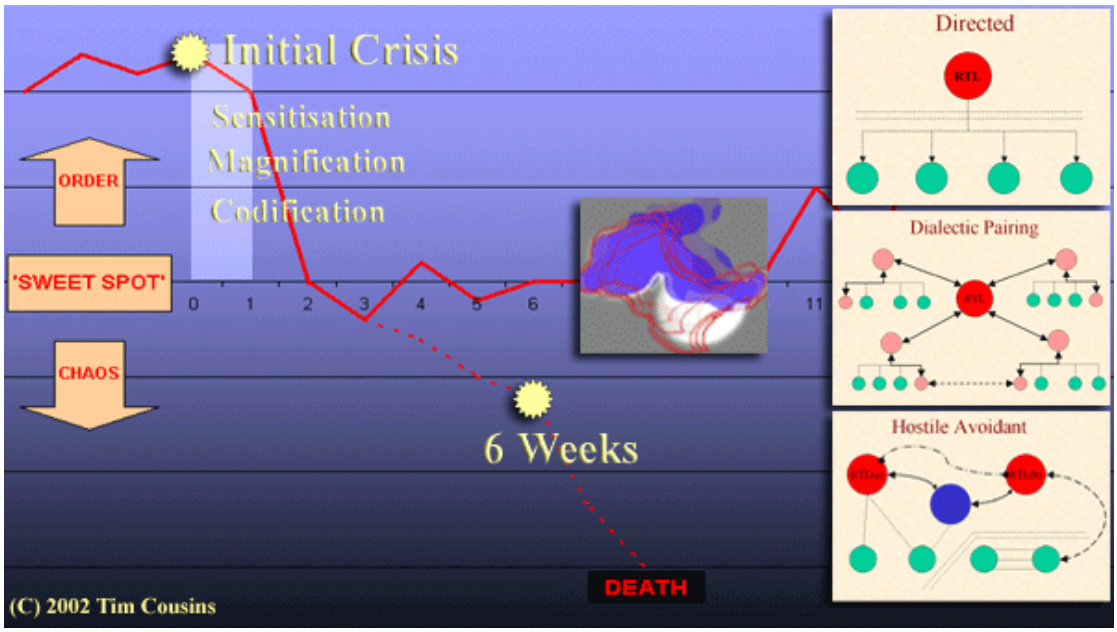


Figure 14 The Recovery Process

By containing anxiety and uncertainty, by providing an independent sounding board for ideas and by maintaining a broad view of the recovery process it is possible to facilitate a balance between the needs of the individual, the organization, the demands of the clean-up and the interests of the stakeholders. This is the sweet spot described by Kaufman (1993), the area of operating which lies between too much order and chaos. This balance in turn facilitates self-regulation and self-organisation without a dictatorial straitjacket.

Recognising and balancing the components of a recovery involves more than just the adherence to a plan for success, though the experience of the planning process gives a clear advantage to an organisation. When there is containment, as well as structures and processes for the sorting of information, the presenting problems will be correctly identified, labelled and creative and effective solutions will emerge from the interactions of the members. Solutions to problems that could never have been anticipated or planned for in the first instance emerge spontaneously. When we see this happening we know that we have engineered an adaptive system.

The work done during the planning process improves the chances of a good recovery. The planning process provides an experience of thinking about the needs of the company in extreme circumstances, as well as engendering a mind-set of preparedness for the unexpected so that in the event, a strategy can be devised. Political differences in individual or company notions of responsibility and territory are encountered when simply playing around with ideas and roles can be rehearsed. Finally, in generating a common story through symbolic processes, a language is built and agreed upon and the whole planning process is integrated into a narrative identity for the group, which provides meaning for the role each person is to play in the event of a recovery effort, particularly in the first few days. The main practical value in the plan itself lies in the attention to the underlying structural needs and the allocation of resources and other requirements.

Disasters will continue to occur even with the best risk management practices. Because of the social and economic costs that arise from a poor or failed recovery we must focus more attention on the recovery phase of a disaster. In particular we need programs to tackle the particular problem of collecting this kind of information but we also need more thinking about what the information means and how it can be used.

Bibliography

Augustine, N 1995, *Managing the Crisis You Tried to Prevent*. Harvard Business Review on Crisis Management, 2000 Harvard Business School Press, Boston.

ANZS 4360:1999 *Risk Management*. Standards Australia Melbourne

Australian National Audit Office, 2000 Business Continuity Management - Keeping the wheels in motion. Australian National Audit Office, Canberra.

Bion, WR 1961. *Experiences in Groups*.Tavistock, London.

Bolman LG and Deal, TE 1997, *Reframing Organizations: Artistry, Choice, and Leadership*, 2nd edn, Jossey-Bass, San Francisco.

Business Continuity Institute (BCI) *THE TEN CERTIFICATION STANDARDS FOR BUSINESS CONTINUITY PRACTITIONERS* <*URL:* http://www.thebci.org/certification_standards.html> *(Accessed <15 May 2002>)*

Clippinger J H III. 1999, *The Biology of Business: Decoding the Natural Laws of Enterprise*, Clippinger ed. Jossey-Bass, San Francisco.

Cousins, TJ 2001, "Claims – The Honest Mistake" *Insurance and Risk Professional Feb – Mar 2002,* McMullan Conway Communications, Australia.

Cousins, TJ 2001, "Sensitization, Magnification and Codification - A Post Loss Process." *The Adjuster, Summer 2001,* KT Journalism, Australia.

< **Cousins, TJ**> <URL:http://www.timcousins.com.au/qualitiesforsurvival.htm> <Qualities for Survival> (Accessed <15 May 2002>)

< **Cousins, TJ**> < URL:http://www.timcousins.com.au/post_loss_recovery_article.htm> <Post Loss Recovery> (Accessed <15 May 2002>)

< **Cousins, T J**> < URL:http://www.timcousins.com.au/staff_tolerance_to_disasters.htm> <Staff Tolerance in Disasters> (Accessed <15 May 2002>)

Cohen, S 1972, *Folk Devils and Moral Panics,* MacGibbon and Kee, London.

Disaster Recovery Institute International 2002 <*Professional Practises for Business Continuity Planners*> <URL: http://www.drii.org/lib/profpractices.pdf> (Accessed <23 June 2002>)

GlobalContinuity.Com *What are the ten key disciplines of business continuity?* <URL:http://www.globalcontinuity.com/Article.asp?id=32868&SessionId=2002623145034&PageSeq=2002623145034&ArtId=11&Type=Knowledge> (Accessed 16 May 2002>)

Holland, JH 1995, *Hidden Order: How Adaptations Build Complexity*. Reading, Addison-Wesley, Mass.

Kauffman, SA 1993, *The Origin of Order: Self-Organization and Selection in Evolution,* Oxford University Press, New York.

Kiel, LD 1994, *Managing Chaos and complexity; A New Paradigm for Managing Change,Innovation, and Organizational Renewal,*. Jossey-Bass, San Francisco.

<Optus v Leighton & Ors [2002] NSWSC 327 para. [1422]> <URL:http://www.timcousins.com.au/optus_v_leighton.htm> <Optus v Leighton & Ors [2002] NSWSC 327> (Accessed <15 May 2002>)

Ortner, S 1973 *On Key Symbols.* American Anthropologist, 1973, 75, 1338-1346

Safetynet 2001 *<The Business Guide to Continuity Management>* <URL: http://www.thebci.org/Guidelines.doc> (Accessed <May 15th 2002>)

Tillett, G 1999, *Resolving Conflict: A Practical Approach 2nd Ed.* Australia: Oxford University Press

UK Dept of Trade and Industry, 1999 *<Business Continuity Management - Preventing Chaos in a Crisis><URL:* http://www.dti.gov.uk/mbp/bpgt/m9ba91001/m9ba910011.html> (Accessed 15 May 2002)

Tim Cousins, born in England and raised in Australia, attended Ballarat Grammar School and was educated at The University of Melbourne and La Trobe University. He taught 'Information Systems Analysis and Design' to both fresher and postgraduate students at Monash University and is currently completing his Masters at Swinburne University.

He has published numerous feature articles, has his own regular column, and is the editor of an Internet-based monthly magazine dedicated to the disaster recovery/risk management professional. He is sought after as a keynote speaker and has a regular spot as a guest lecturer in project management at a Melbourne business school.

Cousins has gained an international reputation through his disaster recovery consulting work and has spoken at a number of international conferences, workshops, and events. He will be speaking at the 12th World Conference on Disaster Management in Toronto in July of this year with a presentation titled "No Plan Survives First Contact With The Enemy" - Key Lessons from a Decade Managing Successful Business Recovery.

Chapter 8 The Disaster Recovery Process Rebuilding Again

How does a business continue after the loss of a building or key facility? The answer to this question is why professional continuity planners are employed in the first place and also why a business owner should never rely on a continuity plan that has neither been reviewed by a business continuity specialist nor has been thoroughly tested by operational and logistical personnel. An Information Technology-only plan will not address the operational and logistical issues surrounding replacement of office furniture, alternate office space, computer equipment, and supplies.

Backup Power Arrangements

All organizations should consider the provision of back-up generators to allow critical business processes to continue when there is a power outage. This decision should be made on a cost justification basis. An Uninterruptible Power Supply System should also be considered for key equipment or services that may be affected by sudden power surges, or where data may be corrupted when the system switches over from main power to a back-up generator. Many UPS systems allow sufficient time for an automated back-up generator to be fired up to replace the lost power.

The recovery plan should note the existence of such back-up generators and UPS systems and the critical functions that they are able to support. The plan should also record the frequency of testing these arrangements and the persons responsible for conducting the tests and maintaining the equipment.

Consultant's note: A former IT manager lamented over the failure of his continuity plan. His company lost over $500,000 because the electricity was out due to a Category Five Tornado that destroyed much of the business community. He had vetoed an alternative generator (cost $9000) because the UPS system that had been installed would carry the equipment 24 hours, and the backup UPS backing up the primary system would carry an additional 12 hours. They never envisioned that electricity would be out for a full seven days.

Recovery of Office and Supplies

The procedure to recover premises, fixtures, and furniture can be collectively referred to as facilities recovery management. The extent of this activity is hard to pre-define, as it will be affected greatly by the actual scale of the emergency. The procedure shown here is given as a guideline that must be reviewed by the organization undertaking the preparation of a business continuity plan to ensure it fits with their own requirements. In many cases, the services of outside specialists may be required to carry out the activity.

ACTIVITIES	RESOURCES REQUIRED	ESTIMATED COMPLETION TIME/DATE
1. Assess damage (see form attached)		
On-site survey of main structures including supports, walls and roof		
Safety issues		
Access problems		
Evaluate re-usability		
Identify further inspections required		
Advise insurance company		
Advise BRT Leader		
2. Assess non-structural damage		
On-site survey of all non-structural facilities		
Determine damage to power, lighting, heating, cooling, and ventilation		
Determine damage to internal partitioning		
Determine damage to doors, windows, and floors		
Determine damage to decoration		
Determine damage to fixtures and fittings		
Determine damage to furniture		
Evaluate recovery period prior to re-occupation		
Advise BRT Leader		
3. Power, lighting, heating, cooling, and ventilation		
Prepare detailed list of damage		
Assess recoverability of each damaged component		
Prepare preliminary specification of repair work or replacement		
Identify availability of suitable vendors		
Determine estimated costs		
Instruct vendors		
Monitor progress		
Advise BRT Leader		
4. Internal partitioning		
Prepare detailed list of damage		
Assess recoverability of each damaged component		
Prepare preliminary specification of repair work or replacement		
Identify availability of suitable vendors		
Determine estimated costs		
Instruct vendors		
Monitor progress		
Advise BRT Leader		
5. Doors, windows and floors		
Prepare detailed list of damage		
Assess recoverability of each damaged component		
Prepare preliminary specification of repair work or replacement		
Identify availability of suitable vendors		

ACTIVITIES	RESOURCES REQUIRED	ESTIMATED COMPLETION TIME/DATE
Determine estimated costs		
Instruct vendors		
Monitor progress		
Advise BRT Leader		
6. Decoration		
Prepare detailed list of damage		
Assess recoverability of each damaged component		
Prepare preliminary specification of repair work or replacement		
Identify availability of suitable vendors		
Determine estimated costs		
Instruct vendors		
Monitor progress		
Advise BRT Leader		
7. Fixtures and fittings		
Prepare detailed list of damage		
Assess recoverability of each damaged component		
Prepare preliminary specification of repair work or replacement		
Identify availability of suitable vendors		
Determine estimated costs		
Instruct vendors		
Monitor progress		
Advise BRT Leader		
8. Furniture		
Prepare detailed list of damage		
Assess recoverability of each damaged component		
Prepare preliminary specification of repair work or replacement		
Identify availability of suitable vendors		
Determine estimated costs		
Instruct vendors		
Monitor progress		
Advise BRT Leader		
9. Identify need for temporary locations		
Assess space required		
Assess period for temporary relocation		
Identify any special requirements		
Contact real estate broker		
Inspect possible temporary sites		
Decide on suitable site		
Prepare site for temporary occupation		
Issue purchase orders for replacement equipment/furniture for damaged items		
10. Relocation to temporary premises		
Notify all affected management and staff of temporary location		
Advise possible period at temporary location		

ACTIVITIES	RESOURCES REQUIRED	ESTIMATED COMPLETION TIME/DATE
Notify customers and suppliers of change of address/contact details		
Arrange transport of undamaged items to temporary premises		
11. Prepare to return to original premises		
Notify all affected management and staff of relocation date		
Notify customers and suppliers of relocation		
Arrange transport of furniture and equipment to original premises		

Alternative Office Furniture

One such outside specialist is Steve Rosen, President of Mark Downs Office Furniture and MDI Contract, one of Maryland's largest office furniture dealerships. Mark Downs specializes in the sale of new, used, and factory seconds in Office Furniture, to include space planning, design, installation, and rental/leasing. Mark Downs's website is www.markdowns.com; their telephone number is 1-800-281-DOWN. Steve learned this information about recovery of office furniture firsthand when, after Hurricane David struck central Maryland in 1979, Mark Downs was under 6 feet of water. Other tropical storms since this event also flooded Mark Downs. His best advice on securing office furniture, other than keep your flood insurance paid at all times, is the following note:

Says Steve:

Some disaster events might require replacement of office furniture. Fires, floods, contamination (asbestos, chemical, biological, radiation), and even earthquakes might require both relocation and the need for temporary or new office furniture.

If a secondary location has been planned, will it be furnished? It's important to pre-identify your needs, and what standards you want. By standards, we mean what quality, colors, styles, and quantity of office furniture you will need, **or be willing to accept.** Traditional desks, executive return desks, executive chairs, computer tables, conference tables, conference chairs, file cabinets (vertical or lateral), and bookcases all have to be identified and colors/fabrics selected.

If your need is temporary, most dealers in the Yellow Pages, listed under "Office Furniture-Renting & Leasing," will require a minimum rental period, usually 90 days. Will the rented items be new or used? Are you willing to settle for used furniture in your space, or will only new products fit in to your plan and budget? See if the renting dealer will apply any portion of the rent towards purchase, in case your needs change.

If your forecasted relocation will last more than one year, you might consider a Lease, which can be much cheaper than rental. In this case, request that the lease be *a true operating lease*, with a residual value of 10 percent; this means that at the end of the lease, you have an option to buy the furniture for 10 percent of its original value. If buying at the end of the lease is not a consideration, then a fair market value lease will have a lower monthly fee, with a higher buy-out figure (which means nothing to you if you are going to walk away from the furniture at the end of the lease).

Do not choose a $1 Buy-Out value; the rates will be much higher, and the cost of the lease may not qualify as an operating expense under IRS guidelines.

When selecting your dealer, make sure you use one that is large enough to serve your needs quickly. Smaller dealers or stationers may not use their own trucks and might not have sufficient inventory to meet your requirements. The larger dealers usually stock enough items to fill your needs, or have access to several wholesalers/distributors that will have large quantities of each desk or chair SKU.

Pre-planning with your designated dealer is important. Picking out styles or colors is too time-consuming after the disaster has hit; the dealer will usually identify your standards, select the proper SKUs, and even help in space planning and layout for no charge. Most dealers will be happy to quote your complete package and have those items already resolved in your disaster recovery plan.

Regular desks and chairs are easy to locate; systems furniture (panels, work surfaces, pedestals, and overstorage units) are much more difficult to locate and supply in a timely manner. Your dealer can help you find out which Systems Manufacturers have Quick-Ship capabilities. And remember, "Quick Ship" to a manufacturer means seven **working** days, plus transportation and set-up delays, not 24 hours like you wanted. There are several refurbishers who can supply used or re-manufactured panels systems quickly; use your dealer to lay out your typical panel configurations ahead of time.

Even if the models and SKUs you selected are discontinued, the dealer will know what price range and quality you want. The larger the order, the more you should expect as a discount from the list prices.

Consider the planning that several World Trade Center companies had in place on September 11th. A law firm relocated to a Manhattan hotel and had the room and bedroom furniture replaced with desks and files.

Larger stock brokerages had full-operating offices set up in New Jersey, complete with furniture, computers, and high-speed Internet lines in place.

Some dealers and manufacturers offered extraordinary efforts in assisting the companies. One manufactory put on 24-hour shifts to produce enough desks and chairs in one weekend to get a company back up. Distributors located 400 desks to meet one company's requirements.

In most cases, pre-planning your specifications and support paid off. Update your specifications annually with your dealer, to see if model numbers or prices have changed. Keep a copy of your contacts, specifications, and contracts for furniture near your contracts for the office space, in your disaster-planning manual.

Consultant Tips for Recovery

Tip 1 – Always keep at least one phone line, such as a fax line or modem line, separate from any other phone systems you may have, such as a PBX. That way you'll have a "back door" available if the phone system fails or the lines into the phone system are disrupted.

Tip 2 – If possible, try to locate communications equipment in more than one location; e.g., phone equipment and telephone company lines in one area and data systems in another. Keep them spaced far enough apart, if possible, to minimize the likelihood of a single point of failure.

Tip 3 – Assuming you have an alternate location (e.g., another office, home, cell phone) to which calls can be routed in an emergency, utilize a service called "remote call forwarding." It's available from the local phone company and redirects incoming calls to your alternate location.

Tip 4 – For a nominal investment of only a few hundred dollars each, uninterruptible power systems (UPS) can provide emergency power to phone systems and network components (e.g., routers). This will help you keep in business long enough to activate your emergency plans.

Tip 5 – Even if your company does not have a formal emergency or disaster plan, at the very least designate an emergency meeting place where all staff are to convene, particularly if the offices must be evacuated. Make sure that information is prominently displayed, e.g., bulletin boards.

Tip 6 – Assuming employees have cell phones, obtain them from at least two different service providers, e.g., Verizon and AT&T. That way if one carrier loses service, the other may still be available.

Tip 7 – For those employees who have PCs at home, ensure they have e-mail and Internet access so they can perform some of their duties at home, if needed.

Tip 8 – Print wallet-sized cards for employees with emergency phone numbers, emergency procedures, and other important instructions to follow in the aftermath of a disaster.

Paul Kirvan, FBCI, CBCP, CISSP
Fortune Consulting
100 Route 36
West Long Branch, NJ 07764
Tel 732-483-2058
Fax 732-483-0112
Mail pkirvan@consultfortune.com
Web www.consultfortune.com

Chapter 9 Information: Key Business Asset or critical liability

There are two types of businesses: Those that have experienced a serious data and connectivity loss and those that will. While most businesses think that they are fully protecting themselves by relying on computer backup systems, this is not the case. On average, 60 percent of all corporate data assets reside on desktop or laptop PCs. Most companies do not have an automated information protection and recovery program for their computers. Most businesses today are connected on the internet in some fashion.

This chapter talks about two risks, the risk to data and the risk to connectivity. The solution to both is a good backup strategy.

Data Loss

The fact is that something will go wrong with every computer in your business at some time, and each of these computers – and their millions of bytes of data – will take time to restore and return to productivity. Whether it's a quick fix, an adhoc system upgrade, or a planned migration, downtime is money lost. And whether it's a virus attack, a hard drive failure, or a stolen laptop, information lost is information compromised. The key causes of data loss are:

- Viruses
- Software Failures
- Application Failures
- File Corruption
- Hard Drive crashes
- Laptop loss/theft
- Natural Disasters
- Power Outages

The tactical results of lost data include:

- Employee downtime
- Clogged Help Desk queues
- Lost productivity
- Compromised information
- Loss of client/customer information

- Increased wear and tear on IT support staff.

Mobile employees are often transporting some of the most critical, timely, and proprietary information known to your business. In fact, PCs at the edge of your business hold 60 percent of your company's corporate information, with much of it going unprotected.

Connected TLM Small-Business Service

Great rates on an easy way to protect your business data and manage your PCs

Prevent data loss from viruses, hackers, hard-drive crashes, power failures, accidental deletions, and other user errors with this enterprise-grade service from the market-leading provider of PC data protection and management solutions. Connected TLM, the global standard in PC data protection, is depended on by more than 400 of the world's largest corporations, including Cisco Systems, Compaq, EMC, GAP, Goodrich, and Hewlett-Packard. Specifically offered to businesses with 5 to 200 PCs – whether desktop, laptop or both* – Connected TLM Small-Business Service:

Provides fast, easy, secure, and fully automated data protection with TLM Backup/Retrieve: hands-off PC backup and easy file restoration.

Ensures rapid, anytime/anywhere system rollback due to virus damage, user error, displaced workers, and lost or stolen computers with TLM Heal.

Allows users to retrieve backed up files from any web browser with iRoam™.

Keeps your PC data secure, your PCs up, and your cost down.

*Not intended for servers or intensive multimedia (see the FAQ for details). Limit of 10GB of backup per individual PC account (seat). Note that most individual PCs contain only 4-6GB of data.

Connected TLM Small-Business Service Features:

- 24/7 access and availability to full-system Backup and Retrieve, Heal and iRoam.
- 112-bit encryption: the industry standard for secure transmission of files encrypts data in transit and in archive - until you restore it on your PC; this ensures complete system state/data protection and full and immediate disaster recovery
- Mirrored servers comply with industry-best practices for high availability and redundancy
- Customer Support: FREE web- and email-based support for administrator and individual users; pay-as-you-go phone support is also available
- View individual PC account usage, history, and configuration
- View summary of, or individual PC accounts
- Find individual PC accounts
- Order CDs of backed-up files

- Automatic file selection: ensures full-system backup and recovery; designed for up to 10GB per individual PC account (temporary files, Internet cache, streaming media and the like are automatically excluded). See FAQ for details.

- Automatic file management: the most recent version of any backed-up file for a particular individual PC account remains in our Data Center; other than the most recent version, files older than 10 versions or 90 days are deleted.

Try Connected TLM Small-Business Service for one month and you'll see why more than 400 of the world's largest companies and over 50,000 PC and laptop users serviced by our Data Center chose Connected TLM.

Connected TLM Data Protection Service allows you to easily protect your data on your PC. It's simple: all you need is a connection to the Internet.

TLM provides an advanced, dependable, convenient, and cost-effective solution for protecting PC-based data and enabling fast and easy data restoration. TLM includes many of the same enterprise capabilities as Connected's corporate solutions to ensure the highest levels of protection and availability of your PC data. Designed specifically to support remote PC and laptop computers, TLM delivers the following benefits:

- Fully automated backups and data restoration for all Windows operating systems

- Optimized for Internet access with line speeds as low as 28.8 Kbps

- State-of-the-art security

- Uses the same technology employed by many Global 2000 companies including Cisco Systems, Compaq, Gap, Goodrich, and more.

Once you have chosen a backup plan that suites your personal needs (see Get Started page) and provided credit card billing information, a small software agent will download to your PC's hard drive. You will automatically start your 30-day FREE trial of backup service. You will not incur any charges for your 30-day trial. After the 30-day trial is complete, simply accept a subscription to continue paid service.

Your data will be compressed, encrypted, and sent over your Internet connection via SSL (secure sockets layer technology), automatically, every day. The information is secured from your PC and stored at an offsite data center in its secure form.

Your privacy is important. Data is never accessed or used for any purpose at the site where it is stored, fully encrypted. Only you have the rights to your data.

Connected TLM Data Protection Service offers two different plans to back up your data.

Critical Data Backup - Protect up to 100MB of PC data files to ensure your data is safe and off site. Only $6.95 per month; credit card required.

Premium Data Backup - Protect up to 4GB of PC data files to ensure your data is safe and off site. Only $14.95 per month; credit card required.

Connectivity Loss

There is one consistent fact about the network connection. It ***will*** go down. The length of time varies, and usually, unless there is some hardware failure of the network router or modem, the length of time varies between hours and days. Usually businesses that depend on the internet have some form of service plan with their Internet Service Provider (ISP) that takes into account what happens when the network fails. There are a lot of factors outside the control of the ISP that cause the network to go down, including cut cables, backbone outages (during the CSX Train Fire in Baltimore, a critical Backbone connection was lost affecting connections up and down the Atlantic coast) and bankruptcy. With the uncertainty of the telecommunications industry, many ISP's notified their customers that within days, their network connections would be shut off permanently, and customers would be left without connectivity, many for up to 50 days without internet or Telephone service.

It is critical to have a backup strategy if your business depends on network connectivity. Figure 1 shows how this backup strategy could work:

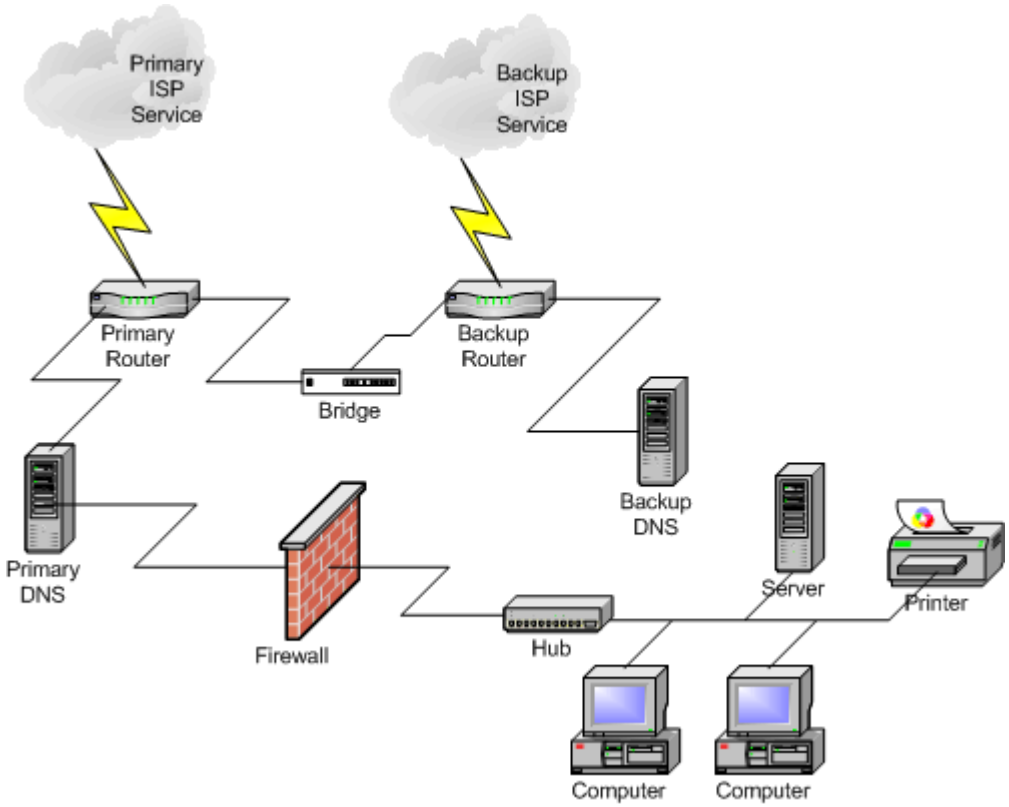


Figure 1. Redundant Network Strategy

In this illustration, a primary router is connected to a primary ISP account, and a backup router is connected to a backup account. The primary account may be the more expensive T1 or dedicated line, the backup account could be a second DSL service with another provider. The second service would only be used if the primary service would stop functioning, so it is not important to have the same bandwidth unless needed. What is shown in this figure is a second Domain Server (DNS) that is referenced by the backup network, so when the primary network goes down, the second DNS server will function and if needed, show the alternate locations of the equipment. The cost of a

second ISP is minimal, but the cost of not having one could be the difference between loosing connectivity for a period of time and loosing business, and surviving the unexpected shutdown by keeping your essential business processes going.

Consultants Notes From The Field

There are simple rules to follow when preserving your data. The first is to backup your data on medium that you can trust. The second rule is to provide some form of redundancy in your backup, either using a remote data center to automatically backup data, or use writeable CD's or tapes to back up critical files, and to make copies and store these copies away from the computer, or in another building, or at home. Even with the best backup systems, the most important rule is sometimes never followed. Backup tapes and media must be tested periodically to ensure that the system that is being backed up can be restored if needed. There is no point in having a backup system if you can't restore the system if it goes down.

Ask yourself the following question. Where do you keep your backup data? If the answer is in the same room as the computer, ask: Is the container at least fireproof? If you are answering no, then it is time to revamp your computer backup strategy before the unexpected shutdown.

APPENDIX A Sample Contingency Plan format

This sample format provides a template for preparing a contingency plan. The template is intended to be used as a guide, and the Contingency Planning Coordinator should modify the format as necessary to meet the system's contingency requirements and comply with internal policies. Where practical, the guide provides instructions for completing specific sections. Text is added in certain sections; however, this information is intended only to suggest the type of information that may be found in that section. The text is not comprehensive and should be modified to meet specific business and system considerations. It is important to note that this is a guide, and should only be used as a guide. Each plan is unique to the business. Please feel free to contact any one of the consultants who contributed to this guidebook for help in completing a functional plan. This section is taken from NIST special publication 800-34, Contingency *Planning Guide for Information Technology Systems*.

1 INTRODUCTION

1.1 Purpose

This *{system name}* Contingency Plan establishes procedures to recover the *{system name}* following a disruption. The following objectives have been established for this plan:

- Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:
  - ***Notification/Activation phase*** to detect and assess damage and to activate the plan
  - ***Recovery phase*** to restore temporary IT operations and recover damage done to the original system
  - ***Reconstitution phase*** to restore IT system-processing capabilities to normal operations.
- Identify the activities, resources, and procedures needed to carry out *{system name}* processing requirements during prolonged interruptions to normal operations.
- Assign responsibilities to designated *{Organization name}* personnel and provide guidance for recovering *{system name}* during prolonged periods of interruption to normal operations.
- Ensure coordination with other *{Organization name}* staff that will participate in the contingency planning strategies. Ensure coordination with external points of contact and vendors who will participate in the contingency planning strategies.

1.2 Scope

1.2.1 Applicability

Various scenarios were considered to form a basis for the plan, and multiple assumptions were made. The applicability of the plan is predicated on two key principles:

- *The {Organization name}'s* facility in *City, State,* is inaccessible; therefore, *{Organization name}* is unable to perform *{system name}* processing for the *Departmen*t.
- A valid contract exists with the *Alternate site* that designates that site in *City, Stat*e, as the *{Organization name}'s* alternate operating facility.
    - *{Organization name}* will use the *Alternate site* building and information technology resources to *recover {system name} functionality* during an emergency situation that prevents access to the *original facilit*y.
    - The designated computer system at the *Alternate site* has been configured to begin processing *{system name} informatio*n.
    - The *Alternate site* will be used to continue *{system name}* recovery and processing throughout the period of disruption, until the return to normal operations.

1.2.2 Assumptions

Based on these principles, the following assumptions were used when developing the IT Contingency Plan:

- The *{system name}* is inoperable at the *{Organization name}* computer center and cannot be recovered within *48 hours.*
- Key *{system name}* personnel have been identified and trained in their emergency response and recovery roles; they are available to activate the *{system name}* Contingency Plan.
- Preventive controls (e.g., generators, environmental controls, waterproof tarps, sprinkler systems, fire extinguishers, and fire department assistance) are fully operational at the time of the disaster.
- Computer center equipment, including components supporting *{system name}*, are connected to an uninterruptible power supply (UPS) that provides *45 minutes to 1 hour* of electricity during a power failure.
- *{System name}* hardware and software at the *{Organization name} original site* are unavailable for at least *48 hours.*
- Current backups of the application software and data are intact and available at the *Offsite storage facility.*
- The equipment, connections, and capabilities required to operate *{system name}* are available at the *Alternate site* in *City, State.*
- Service agreements are maintained with *{system name}* hardware, software, and communications providers to support the emergency *system* recovery.

The *{system name}* Contingency Plan does not apply to the following situations:

- **Overall recovery and continuity of business operations.** The Business Resumption Plan and Continuity of Operations Plan (COOP) are appended to the plan.
- **Emergency evacuation of personnel.** The Occupant Evacuation Plan is appended to the plan.
- *Any additional constraints should be added to this list.*

1.3 Authority/References

This *{system name}* Contingency Plan complies with the *{Organization name}'s* IT contingency planning policy as follows:

"THE ORGANIZATION SHALL DEVELOP A CONTINGENCY PLANNING CAPABILITY TO MEET THE NEEDS OF CRITICAL SUPPORTING OPERATIONS IN THE EVENT OF A DISRUPTION EXTENDING BEYOND 72 HOURS. THE PROCEDURES FOR EXECUTION OF SUCH A CAPABILITY SHALL BE DOCUMENTED IN A FORMAL CONTINGENCY PLAN AND SHALL BE REVIEWED AT LEAST ANNUALLY AND UPDATED AS NECESSARY. PERSONNEL RESPONSIBLE FOR TARGET SYSTEMS SHALL BE TRAINED TO EXECUTE CONTINGENCY PROCEDURES. THE PLAN, RECOVERY CAPABILITIES, AND PERSONNEL SHALL BE TESTED TO IDENTIFY WEAKNESSES OF THE CAPABILITY AT LEAST ANNUALLY."

Record of Changes

Modifications made to this plan since the last printing are as follows:

Record of Changes			
Page No.	Change Comment	Date of Change	Signature

2 CONCEPTS OF OPERATIONS

2.1 System Descriptions and Architecture

Provide a general description of system architecture and functionality. Indicate the operating environment, physical location, general location of users, and partnerships with external organizations/systems. Include information regarding any other technical considerations that are important for recovery purposes, such as backup procedures. Provide a diagram of the architecture, including security controls and telecommunications connections.

2.2 Responsibilities

The following teams have been developed and trained to respond to a contingency event affecting the IT system.

The Contingency Plan establishes several teams assigned to participate in recovering *{system name}* operations. The *{team name}* is responsible for recovery of the *{system name}* computer environment and all applications. Members of the *team name* include personnel who are also responsible for the daily operations and maintenance of *{system name}*. The *team leader title* directs the *{team name}*.

Continue to describe each team, their responsibilities, leadership, and coordination with other applicable teams during a recovery operation.

The relationships of the team leaders involved in *system* recovery and their member teams are illustrated in Figure XX below.

(Insert hierarchical diagram of recovery teams. Show team names and leaders; do not include actual names of personnel.)

Describe each team separately, highlighting overall recovery goals and specific responsibilities. Do not detail the procedures that will be used to execute these responsibilities. These procedures will be itemized in the appropriate phase sections.

3 NOTIFICATION AND ACTIVATION PHASE

This phase addresses the initial actions taken to detect and assess damage inflicted by a disruption to *{system name}*. Based on the assessment of the event, the plan may be activated by the *Contingency Planning Coordinato*r.

In an emergency, the *{Organization name}'s* top priority is to preserve the health and safety of its staff before proceeding to the Notification and Activation procedures.

Contact information for key personnel is located in Appendix A. The notification sequence is listed below:

- The first responder is to notify the *Contingency Planning Coordinato*r. All known information must be relayed to the *Contingency Planning Coordinator.*
- The *systems manager* is to contact the *Damage Assessment Team Leader* and inform them of the event. The *Contingency Planning Coordinator* is to instruct the Team Leader to begin assessment procedures.
- The *Damage Assessment Team Leader* is to notify team members and direct them to complete the assessment procedures outlined below to determine the extent of damage and estimated recovery time. If damage assessment cannot be performed locally because of unsafe conditions, the *Damage Assessment Team* is to follow the outline below.

Damage Assessment Procedures:

(Detailed procedures should be outlined to include activities to determine the cause of the disruption; potential for additional disruption or damage; affected physical area and status of physical infrastructure; status of IT equipment functionality and inventory, including items that will need to be replaced; and estimated time to repair services to normal operations.)

- Upon notification from the *Contingency Planning Coordinator,* the *Damage Assessment Team Leader* is to …
- *The Damage Assessment Team* is to ….

Alternate Assessment Procedures:

- Upon notification from the *Contingency Planning Coordinator,* the *Damage Assessment Team Leader* is to …
- *The Damage Assessment Team* is to ….
    - When damage assessment has been completed, the *Damage Assessment Team Leader* is to notify the *Contingency Planning Coordinator* of the results.
    - The *Contingency Planning Coordinator* is to evaluate the results and determine whether the contingency plan is to be activated and if relocation is required.
    - Based on assessment results, the *Contingency Planning Coordinator* is to notify assessment results to civil emergency personnel (e.g., police, fire) as appropriate.

The Contingency Plan is to be activated if one or more of the following criteria are met:

1. *{system name}* will be unavailable for more than 48 hours
2. *Facility is damaged and will be unavailable for more than 24 hours*
3. *Other criteria, as appropriate.*

- If the plan is to be activated, the *Contingency Planning Coordinator* is to notify all Team Leaders and inform them of the details of the event and if relocation is required.
- Upon notification from the *Contingency Planning Coordinato*r, Team Leaders are to notify their respective teams. Team members are to be informed of all applicable information and prepared to respond and relocate if necessary.
- The *Contingency Planning Coordinator* is to notify the *Offsite storage facility* that a contingency event has been declared and to ship the necessary materials (as determined by damage assessment) to the *Alternate site.*
- The *Contingency Planning Coordinator* is to notify the *Alternate site* that a contingency event has been declared and to prepare the facility for the *Organization's* arrival.
- The *Contingency Planning Coordinator* is to notify remaining personnel (via notification procedures) on the general status of the incident.

4 RECOVERY OPERATIONS

This section provides procedures for recovering the application at the alternate site, whereas other efforts are directed to repair damage to the original system and capabilities.

The following procedures are for recovering the *{system name}* at the *Alternate Site.* Procedures are outlined per team required. Each procedure should be executed in the sequence in which it is presented to maintain efficient operations.

Recovery Goal. *State the first recovery objective as determined by the Business Impact Assessment (BIA). For each team responsible for executing a function to meet this objective, state the team names and list their respective procedures.*

- *{team name}*
  - *Team Recovery Procedures*
- *{team name}*
  - *Team Recovery Procedures*
- *{team name}*
  - *Team Recovery Procedures*

Recovery Goal. *State the second recovery objective as determined by the BIA. For each team responsible for executing a function to meet this objective, state the team names and list their respective procedures.*

- *{team name}*
  - *Team Recovery Procedures*
- *{team name}*
  - *Team Recovery Procedures*
- *{team name}*
  - *Team Recovery Procedures*

Recovery Goal. *State the remaining recovery objectives (as determined by the BIA). For each team responsible for executing a function to meet this objective, state the team names and list their respective procedures.*

5 RETURN TO NORMAL OPERATIONS

This section discusses activities necessary for restoring *{system name}* operations at the *{Organization name}'s* original or new site. When the computer center at the original or new site has been restored, *{system name}* operations at the *Alternate site* must be transitioned back. The goal is to provide a seamless transition of operations from the *Alternate site* to the computer center.

Original or New Site Restoration

Procedures should be outlined, per necessary team, to restore or replace the original site so that normal operations may be transferred. IT equipment and telecommunications connections should be tested.

- *{team name}*
  - *Team Recovery Procedures*
- *{team name}*
  - *Team Recovery Procedures*
- *{team name}*
  - *Team Recovery Procedures*

5.1 Concurrent Processing

Procedures should be outlined, per necessary team, to operate the system in coordination with the system at the original or new site. These procedures should include testing the original or new system until it is functioning properly and the contingency system is shut down gracefully.

- *{team name}*
  - *Team Recovery Procedures*
- *{team name}*
  - *Team Recovery Procedures*
- *{team name}*
  - *Team Recovery Procedures*

5.2 Plan Deactivation

Procedures should be outlined, per necessary team, to clean the alternate site of any equipment or other materials belonging to the organization, with a focus on handling sensitive information. Materials, equipment, and backup media should be properly packaged, labeled, and shipped to the appropriate location(s). Team members should be instructed to return to the original or new site.

- *{team name}*
  - *Team Recovery Procedures*
- *{team name}*
  - *Team Recovery Procedures*
- *{team name}*
  - *Team Recovery Procedures*

6 PLAN APPENDICES

The appendices included should be based on system and plan requirements.

- *Personnel Contact List*
- *Vendor Contact List*
- *Equipment and Specifications*
- *Service Level Agreements and Memoranda of Understanding*
- *IT Standard Operating Procedures*
- *Business Impact Analysis*
- *Related Contingency Plans*
- *Emergency Management Plan*
- *Occupant Evacuation Plan*
- *Continuity of Operations Plan.*

APPENDIX B Sample Business Impact Analysis and Template

In this example, a business maintains a small field office with a local area network (LAN) that supports approximately 50 users. The office relies on the LAN and its components for standard automated processes, such as developing and using spreadsheets, word processing, and electronic mail (e-mail). The office also maintains a customized database application that supports Inventory, a key resource management process. The network manager is responsible for developing a LAN contingency plan and begins with the BUSINESS IMPACT ANALYSIS.

The LAN includes the following components:

- Authentication/network operating system server
- Database server (supports customized Inventory database application)
- File server (stores general, non-Inventory files)
- Application server (supports office automation software)
- Networked printer
- E-mail server and application
- 50 desktop computers
- Five hubs.

The Contingency Planning Coordinator begins the BUSINESS IMPACT ANALYSIS process by identifying the network stakeholders. In this case, the coordinator identifies and consults with the following individuals:

- Field office manager
- Inventory process manager
- Sampling of network users
- System administrators for each network server.

Based on subsequent discussions, the coordinator learns the following information:

- The Inventory system is critical to the parent agency's master resource management operations; the system provides updated data to the larger system at the end of each business day. If the system were unavailable for more than one working day (eight hours), significant business impacts would result at the parent agency. Inventory requires a minimum of five personnel with desktop computers and access to the system database to process data.

- Other non-Inventory processes may be considered noncritical and could be allowed to lapse for up to ten days.

- The field office manager and Inventory manager indicate that e-mail is an essential service; however, staff can operate effectively without e-mail access for up to three days.

- Staff could function without access to the spreadsheet application for up to 15 working days without affecting business processes significantly. Word processing access would need to be restored within five working days; however, individuals could use manual processes for up to ten days if the required forms were available in hard-copy format.

- Outputs from the day's Inventory system records normally are printed daily; the data to be printed may be stored on any desktop computer used by the Inventory system staff. In an emergency, the Inventory system output could be transmitted electronically via e-mail for up to three days before significantly affecting business operations. Other printing functions would not be considered essential and could be unavailable for up to ten days with no impact on business functions.

Based on the information gathered in discussions with stakeholders, the Contingency Planning Coordinator follows the three-step BUSINESS IMPACT ANALYSIS process to identify critical information technology (IT) resources, identify outage impacts and allowable outage times, and develop recovery priorities.

Identify Critical IT Resources

The manager identifies the following resources as critical, meaning that they support critical business processes:

- Authentication/network operating system server (required for users to have LAN access)
- Database server (required to process the Inventory system)
- E-mail server and application
- Five desktop computers (to support five Inventory users)
- One hub (to support five Inventory users)
- Network cabling
- Electric power
- Heating, Ventilation, and Air Conditioning (HVAC)
- Physical security
- Facility.

Identify Outage Impacts and Allowable Outage Times

Next, the manager determines outage impacts and allowable outage times for the critical resources:

Resource	Outage Impact	Allowable Outage Time
Authentication server	Users could not access Inventory system	8 hours
Database server	Users could not access Inventory system	8 hours
E-mail server	Users could not send e-mail	2 days
5 desktop computers	Users could not access Inventory system	8 hours
Hub	Users could not access Inventory system	8 hours
Network cabling	Users could not access Inventory system	8 hours
Electric power	Users could not access Inventory system	8 hours
Printer	Users could not produce Inventory reports	4 days

Develop Recovery Priorities

Using the table completed in the previous step, the Contingency Planning Coordinator develops recovery priorities for the system resources. The manager uses a simple high, medium, low scale to prioritize the resources. High priorities are based on the need to restore critical resources within their allowable outage times; medium and low priorities reflect the requirement to restore full operational capabilities over a longer recovery period.

Resource	Recovery Priority
Authentication server	High
Database server	High
5 desktop computers	High
1 hub	High
Network cabling	High
Electric power	High
E-mail server	Medium
Printer	Medium
Remaining desktop computers (45)	Low
Remaining hubs (4)	Low

Having completed the BUSINESS IMPACT ANALYSIS, the Contingency Planning Coordinator may use the recovery priority information above to develop recovery strategies that enable the network to be recovered in a prioritized manner, with all system resources being recovered within their respective allowable outage times.

A template for completing the BUSINESS IMPACT ANALYSIS is provided on the following page.

Business Impact Analysis Template

This sample template is designed to assist the user in performing a BUSINESS IMPACT ANALYSIS on an IT system. The BUSINESS IMPACT ANALYSIS is an essential step in developing the IT contingency plan. The template is meant only as a basic guide and may not apply to all systems. The user may modify this template or the general BUSINESS IMPACT ANALYSIS approach as required to best accommodate the specific system.

Preliminary System Information

Organization:	Date BUSINESS IMPACT ANALYSIS Completed:
System Name:	BUSINESS IMPACT ANALYSIS POC:
System Manager POC:	
System Description: *{Discussion of the system purpose and architecture, including system diagrams}*	

A. Identify System Points of Contact	**Role**
Internal {Identify the individuals, positions, or offices *within* your organization that depend on or support the system; also specify their relationship to the system}	
○ ○ ○	○ ○ ○
External {Identify the individuals, positions, or offices *outside* your organization that depend on or support the system; also specify their relationship to the system}	
○ ○ ○	○ ○ ○

B. Identify System Resources *{Identify the specific hardware, software, and other resources that comprise the system; include quantity and type}*
Hardware ○ ○
Software ○
Other resources

○

C. Identify critical roles {List the roles identified in Section A that are deemed critical}
○ ○ ○ ○ ○

D. Link critical resources to critical roles {Identify the IT resources needed to accomplish the roles listed in Section C}	
Critical Role	**Resources** ○ ○ ○
	○ ○ ○
	○ ○ ○

E. Identify outage impacts and allowable outage times {Characterize the impact on critical roles if a critical resource is unavailable; also, identify the maximum acceptable period that the resource could be unavailable before unacceptable impacts resulted}		
Resource	**Outage Impact**	**Allowable Outage Time**

F. Prioritize resource recovery {List the priority associated with recovering a specific resource, based on the outage impacts and allowable outage times provided in Section E. Use quantitative or qualitative scale (e.g., high/medium/low, 1-5, A/B/C)}	
Resource	**Recovery Priority**

APPENDIX C Glossary

Backup: A copy of files and programs made to facilitate recovery if necessary.

Business Continuity Plan (BCP): The documentation of a predetermined set of instructions or procedures that describe how an organization's *business functions* will be sustained during and after a significant disruption.

Business Impact Analysis (BIA): An analysis of an IT system's requirements, processes, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.

Business Recovery/Resumption Plan (BRP): The documentation of a predetermined set of instructions or procedures that describe how *business processes* will be restored after a significant disruption has occurred.

Cold Site: A backup facility that has the necessary electrical and physical components of a computer facility, but does not have the computer equipment in place. The site is ready to receive the necessary replacement computer equipment in the event that the user has to move from their main computing location to an alternate site.

Computer: A device that accepts digital data and manipulates the information based on a program or sequence of instructions for how data is to be processed.

Contingency Plan: Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster.

Contingency Planning: See Contingency Plan.

Continuity of Operations Plan (COOP): A predetermined set of instructions or procedures that describe how an organization's *essential functions* will be sustained for up to 30 days as a result of a disaster event before returning to normal operations.

Disaster Recovery Plan (DRP): A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities.

General Support System*:* An interconnected information resource under the same direct management control that shares common functionality. It usually includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications. Individual applications support different mission-related functions. Users may be from the same or different organizations.

Hot Site: A fully operational offsite data processing facility equipped with both hardware and system software to be used in the event of a disaster.

Incident Response Plan: The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber attacks against an organization's IT system(s).

Major Application: An application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, unauthorized access to, or modification of, the information in the application. A breach in a major application might comprise many individual application programs and hardware, software, and telecommunications components. Major applications can be either a major software application or a combination of hardware/software where the only purpose of the system is to support a specific mission-related function.

Mobile Site: A self-contained, transportable shell custom-fitted with the specific IT equipment and telecommunications necessary to provide full recovery capabilities upon notice of a significant disruption.

Reciprocal Agreement: An agreement that allows two organizations to back each other up.

Risk Management: The ongoing process of assessing the risk to mission/business as part of a risk-based approach used to determine adequate security for a system by analyzing the threats and vulnerabilities and selecting appropriate, cost-effective controls to achieve and maintain an acceptable level of risk.

System: A generic term used for briefness to mean either a major application or a general support system.

System Development Life Cycle: The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation.

Warm Site: An environmentally conditioned workspace that is partially equipped with IT and telecommunications equipment to support relocated IT operations in the event of a significant disruption.