# Business Continuity in Communications

FOR

DUMMIES®

AVAYA LIMITED EDITION

by Greg Gilbert


Wiley Publishing, Inc.

**Business Continuity in Communications For Dummies®, Avaya Limited Edition**

Published by
**Wiley Publishing, Inc.**
111 River Street
Hoboken, NJ 07030-5774
www.wiley.com



Published by Wiley Publishing, Inc., Indianapolis, Indiana

Published simultaneously in Canada



ISBN-13: 978-0-470-03982-3

ISBN-10: 0-470-03982-5

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

1O/SY/QS/QW/IN

## Publisher's Acknowledgments

We're proud of this book; please send us your comments through our online registration form located at www.dummies.com/register/.

Some of the people who helped bring this book to market include the following:

***Acquisitions, Editorial, and Media Development***

**Project Editor:** Blair J. Pottenger

**Executive Editor:** Gregory Croy

**Senior Copy Editor:** Barry Childs-Helton

**Business Development Representative:** Jackie Smith

**Editorial Manager:** Kevin Kirschner

***Composition Services***

**Project Coordinator:** Kristie Rees

**Layout and Graphics:** Julie Trippetti

**Proofreader:** Amanda Briggs

***Special Help***

Millicent Barksdale, Doug D'Angelo, Steve Hailey, Lisa Kluberspies, Reinhard Koch, Jim Mannion, Catherine McNair, Patti Moran, Howard Peace

---

**Publishing and Editorial for Technology Dummies**

**Richard Swadley,** Vice President and Executive Group Publisher

**Andy Cummings,** Vice President and Publisher

**Mary Bednarek,** Executive Acquisitions Director

**Mary C. Corder,** Editorial Director

**Publishing for Consumer Dummies**

**Diane Graves Steele,** Vice President and Publisher

**Joyce Pepple,** Acquisitions Director

**Composition Services**

**Gerry Fahey,** Vice President of Production Services

**Debbie Stailey,** Director of Composition Services

# Table of Contents

# Introduction

*Business continuity* is a collection of disciplines that are closely related and often confused with each other. Disaster management, disaster recovery, crisis management, business recovery, emergency planning, and business continuity are all frequently spoken of in the same breath like siblings or close cousins. The topic of business continuity has, by default, come to represent this collection of disciplines. We will call this collection BCDR, which literally stands for Business Continuity and Disaster Recovery, but which represents the full spectrum.

Communications is often the critical focus of many types of management problems and concerns. Business continuity in communications is essential as it represents that set of solutions supporting the assurance that communications will remain functional and effective when business continuity is the problem at hand. If communications is such a critical focus point, then we must understand that it is indeed the area where we can experience the most problems and waste the most effort and money. When dealing with unsolved communication problems, we come away more badly beaten than when dealing with any other problems.

Communications is an ongoing part of our daily lives and we take it and its many forms of technology for granted. We dial the phone, send the e-mail, order services from the web page, listen to satellite-bounced conversations, and use complex programs to play electronic games. All of these wondrous abilities are evolved out of technologies that are communications based and communications driven.

Business continuity has become a core focus in many companies and countries throughout the world, and there are now laws dictating the needs and parameters for these standards.

# The Avaya Advantage

Business continuity requires uncompromised communications at all times. The technology and professional services supporting communications have virtually exploded over the years and this exponential growth has also become part of our daily expectations. In order to realize those daily expectations on an ongoing basis, a company must know the terrain and have the weaponry to do battle with the dragons that live there.

Avaya is the preeminent market leader in the business continuity arena as far as communications is concerned. Avaya uses its intimate understanding of business continuity needs to bring real-world solutions to sticky problems in a timely and cost-effective framework. You might think that Avaya has a crystal ball when it comes to intuitive problem solving. Their approach to business continuity takes normal problem solving to the next level with their professional use of risk assessment, business impact analysis, and communications-born solutions. Their highly developed and successful plans and operations have established them as such a major force that companies seek them out for business continuity solutions as well as communications system needs.

With the telecommunications market loaded with so much competition, it is easy to see why Avaya stands head and shoulders above the rest. Avaya is a multi-talented market leader. To understand what it means to be a real leader in the communications market, you also need to understand things like the significance of converging your traditional telephony systems onto your computer network for IP Telephony. You also need to understand things like communications systems and program features. In short, you need to know how to work the telephone beyond just picking it up to answer or dialing nine for an outside line. If you want to do things like create an enterprise-wide communications network, or design a backup communications system that is worldwide and seamless to users and customers, you need to be talking to Avaya. And you don't have to throw the baby out with the wash water. You don't need to trash your investments made in other communications systems' hardware. You can do it the Avaya way.

Avaya has *VoIP* (Voice over Internet Protocol), which is a new technology that uses the Internet for telephone calls. This is

also a good backup when hard-line systems are down. In the IP Telephony world, an Avaya system includes all the features you are familiar with—voicemail, call waiting, and call forwarding, to name a few. Avaya also has intuitive call center–oriented systems which help their customers solve their most likely problems with one phone call using artificial intelligence and specific customer trend analysis. This is like going to your favorite restaurant and the server knowing who you are and asking, "Would you like your usual today?"

Avaya represents a solid gold relationship with communications as well as business continuity. My goal here is to provide a reference that anybody can use to approach, understand, address, and survive the pitfalls of disasters, emergencies, and crises. And, as a caveat, along the way you will also see how this applies to the discipline of business communications. Communications has always been an area where you can lose your shirt if you fail to do things right. Avaya has survived this storm and has also provided valuable input into the development of this book and its communications focus.

In this book, you will learn why companies are motivated to say things like, "Most fundamentally, though, Avaya has given us a business continuity process and baseline that forms the foundation of all our future efforts. The Avaya assessment has definitely given us control over the business that we didn't have before." Visit Avaya.com to find out more.

# About This Book

If you are a manager who needs to decide what to do in the face of starting a business continuity program, making a budget, and considering technology such as VoIP (Voice Over Internet Protocol), or if you are an IT person looking to help your boss make an informed decision about integrated networking, designing the next level of a communications strategy, this book provides an excellent place for you to begin. This book also provides an excellent starting place for end users who are new to business continuity and disaster planning and how things like VoIP and other Avaya systems, software, and services can ease the pain.

This book uses several case studies and hard experiences to explain business continuity and how communications technology such as VoIP works and how it compares to

telecommunications technology that was previously considered irreplaceable. By the time you finish this book, you will understand why many businesses throughout the world have turned to Avaya for their VoIP and integrated networking as their main system for data, voice, and video transfer along with intuitive systems and software designed to save time and keep customers smiling. You may read this book from cover to cover, which is what I recommend, seeing as it's a pretty fast read. If you are in a hurry, however, give it a quick skim and note the primary headings. Feel free to dip into whatever part or section catches your interest and best suits your needs and then return to the rest of the book when you have more time to enjoy the read.

# How This Book Is Organized

Each part of this book focuses on a different aspect of business continuity and the communications arena. As I mentioned, you may choose to read the book cover to cover, or skip around to find the information you need when you need it. I recommend a full read or at least an initial good skim of all primary highlights in order to gain a more complete understanding.

## Part I: What Communications Can Do for Business Continuity

Part I introduces you to the basics of business continuity. You get the rundown on essential terms, the language of business continuity, and the general workings of the concepts. This will provide you with a lay of the land around business continuity as the terrain is treacherous. This part also includes the first of several sidebars (those funky gray boxes with text in them). These sidebars outline case studies that help you see some real-world applications of the technology. They're really great, so check them out.

## Part II: Developing Risk Management for Your Business

In Part II, you discover how a detailed understanding of business continuity is contingent upon security-type thinking:

prevention. Preventing problems before they become problems can reduce your operating costs — and the effect is immediate. To help set business continuity in context, Part II takes you deeper into the jungle of business continuity, showing you detailed analyses such as the Business Impact Analysis (BIA). You will also see a case study on VoIP showing how the technology can be used to address a disaster scenario. I will let Part II speak for itself, but after reading it you will understand that in the long run, Avaya is the most cost-effective choice for your communications decisions. You will also note specifically that the new VoIP (Voice over Internet Protocol) is worth a good hard look, especially concerning BCDR planning.

## Part III: Implementing Your BCP (Business Continuity Plan)

Part III outlines the management planning, organizing, implementing, and controlling required to perform well in any management situation. With detailed support from a case study involving San Francisco Airport and a masterful approach to the use of the technology available from Avaya, you are treated to an understanding of business continuity that provides successful strategies, lowered risk assessments, and reduced budgetary strains.

## Part IV: Top Ten Reasons to Develop a Business Continuity Plan

The reasons to switch to Avaya and to some of the newer technology such as VoIP are countless, depending on how far you want to project the future of the marketplace. Part IV describes the ten best reasons to make sure you develop a viable business continuity plan and not just design a pretty book for the shelf. You will understand that embracing the available technology, such as VoIP, can make a real difference. The use of powerful communications tightens your overall business continuity focus and your business success because it relates to all aspects of the business. This relationship covers everything from projections for the future of your business to use of the telephony industry to enhance your profits and speed up the success moves of your organization.

## Glossary and Acronyms

The Business Continuity Disaster Recovery (BCDR) landscape is loaded with acronyms and new definitions for words where we think we already have good definitions. These words, definitions, and cryptic acronyms have been assimilated and adapted from a host of sources including my own prolific imagination. This section will allow you to make sense of it all.

# Icons Used in This Book

This book uses icons to highlight certain paragraphs and to alert you to particularly useful information. Here's a rundown of what those icons mean:


A Tip icon denotes critical points, key facts, sit-up-and-take-notice items which will add to the understanding of concepts, promotion of clearer thoughts, and better overall handling of information.


A Warning icon indicates treacherous territory that has made mincemeat out of lesser mortals who have come before you. Skip this point at your own peril. Beware of the dragons.


A Technical Stuff icon represents information that you may skip or read. The choice is yours. You will fill your head with more stuff that may prove valuable as you expand your understanding of Business Continuity Disaster Recovery (BCDR). You do risk overdosing on stuff you may not need right away. Be prepared to come back and read it if you choose to skip it at the outset.


The Remember icon points out things that I may already covered but that bear repeating. Now, I have never in my life actually tied a string around my finger. But there are times when I should have. Some things we do indeed need to remember. Forget it and you're going to really get into trouble.

# Part I

# What Communications Can Do for Business Continuity

### In This Part

- Nailing the basics of business continuity
- Grounding BCDR in real-world issues
- Figuring out where to go for help
- Handling the Workers' Compensation Fund (a case study)

Business is all about priorities; sometimes those priorities get a little out of whack. For instance, you might be surprised at the long hours spent arguing the semantics of Business Continuity and Disaster Recovery (BCDR) — which is (in effect) the formal study of how to make sure your business can keep on keepin' on. The groups tasked with actually warding off disaster often haggle over the title of their group, or sweat to come up with a catchy title for the article they're writing. The sad truth is that the English language has no neat one, two, or three words that adequately define what you have to do to keep your business going in the real world (which is, too often, not a safe world). However you define business continuity, the work has to be done.

## BCDR: One Problem, Many Facets

Business Continuity and Disaster Recovery (BCDR) is fairly complex, but it can seem more tangled than it is. It's a multidisciplinary response to a problem that can come at you from many directions. So let's take a closer look at what makes up

the landscape here — the six groups of business processes that make up BCDR.

Flip through the "Glossary and Acronyms" section at the back of this book to make sure you've nailed the terminology from the outset.

- **Business continuity:** These processes aim to keep an enterprise operational in spite of potentially damaging incidents. The operating assumption here is that business continues and does not actually stop as a result of an incident.
- **Business recovery:** These processes assist an enterprise in recovering from an actual incident. They are what must happen if the business did actually stop and its operations must be recovered and restarted.
- **Crisis management:** These processes encompass not only planning to deal with disruptions, but also handling the process of settling an incident as it's happening — and to minimize the ill effects. Every disaster is indeed a crisis, but not every crisis is a disaster.
- **Disaster management:** These processes (usually multidisciplinary) address the problems associated with specific disasters — usually knock-down-drag-out events such as hurricanes, tornadoes, fires, explosions, executive assassinations — that are far more severe than a mere "crisis."

These last two items sound similar, but it's a difference in scale: A building totally destroyed by fire would be a "disaster." A crashed server with a reasonably decent backup is a "crisis" until the data is brought up to speed — but a crashed server *that holds critical data but has no backup* could easily be a "disaster."

- **Disaster recovery:** These processes bring the business back to life after an actual incident, address the effects of the incident, and seek to fix the problems it actually inflicted on the enterprise.
- **Emergency planning:** These processes aim at comprehensive preparedness for a bad situation when it occurs. The goal is readiness and preparedness rather than real-time response and recovery.

Put all that together, and you have a two-part imperative: *Business continuity* is about maintaining the capabilities and data that your business needs to be durable and effective; *disaster recovery* is about being appropriately prepared to bounce back from a real-world hit. Taken together as BCDR, they're about doing what it takes to stay in business despite disruptions — affecting the whole package. When a crisis hits, BCDR is more about action than talk. Between crises, it's about knowing what to prepare for.

Granted, BCDR can get a bit complex, but a hasty plan — based on only a partial glimpse of what's involved — can be even more dangerous than wading into a crisis without a clue. Why? Because half-baked disaster scenarios provide a false sense of security, based on unrealistic assessments of

- What measures work well to prevent specific problems
- What measures have proven totally ineffective
- What measures are appropriate for an incident already in progress

The worst effect of such inaccuracy is to play down the severity of the situation — by refusing to look at the devil in the details. This shortsightedness is most prevalent in harried senior executives who don't have time for what they see as sweating the small stuff. Too often, they only want to deal with the big picture — forgetting that the view from 30 thousand feet is never as bad as what you see at Ground Zero — where the real damage (and real lesson) is.

So tie on that bandana: This part selectively sweats the "small" stuff. The goal is to make sure we really understand what business continuity is — and why the whole world is getting so excited about it. And since most problems are best addressed with some form of communications, we want to keep communications at the ready while we dig into these details.

# Business Continuity at Stake

"Business continuity" sounds so matter-of-fact — isn't most of the stuff you have to do to protect it just common sense? Well, not exactly. Even if common sense were all that common — and in practice, it isn't — the basics of business continuity are

a bit complex. Without a good grounding in what can actually happen (specific, real-world events) — and an equally clear understanding of how the emotional brouhaha of an incident can block a solution — we remain at the mercy of the incident. And that's worse than having no plan.

The yikes-here-it-comes terribleness that sweeps over us when we're subjected to situations that evoke strong emotion has one reliable effect: Our ability to think clearly and accurately goes out the window. Most people do not make good decisions when they're crying, yelling unprintable words, or otherwise getting too agitated to process information correctly. So okay, keep a crying towel handy — but study up on what can actually happen before you have to use it.

## How does communications fit in?

So here are the six disciplines that cover the essential bases of BCDR, with their basic goals and wearing their communications raincoat and galoshes.

- **Business continuity:** Keep the business running, regardless. Communications helps you weather the storm. An alternate means of maintaining telecommunications (phone service) like VoIP can make your crashed phone system totally transparent to your customers.
- **Business recovery:** Get back up to speed after an incident. Communications speeds the bounce-back and gets the word out that you're still in the game. Communications contingencies such as self-diagnosing servers that transfer their functions over to a backup automatically minimize what otherwise would be a major failure.
- **Crisis management:** Prepare to handle an incident efficiently. Communications makes the measures more effective. Having an intuitive operating system running the phones means that you are already two steps ahead in anticipating what your customers are going to need when they dial you up.
- **Disaster management:** Prepare to handle a disaster efficiently. Communications makes the preparation uniform. If an incident is already being called a disaster, it means

that the fan is already covered in muck and we are going to require a well constructed communication system to stand up to the abuse of a 300% increase in use over the next 72 hours. Communications and software systems are already the life blood of many companies. Everything else can die on the vine at the outset of an incident, but the phones must work.

- **Disaster recovery:** Revive and repair the business after an incident. Communications coordinates the effort. Okay, we cleaned most of the muck off the fan. Now we need to use our communications resources to perform the fixing and keep everyone in the loop and not waste time trying to use a bunch of strange numbers and goofy telephone codes.
- **Emergency planning:** Be realistically (but thoroughly) prepared. Communications keeps everybody on the same page. Good communications is just that. It is the proper transmission of solid information over uncompromised channels to accurate and designated targets. Sounds like a war tactic doesn't it? Emergency planning is indeed preparation for war.

## From details to big picture — and back

Bottom line, doing effective BCDR means creating a multidisciplinary, multifaceted approach to a complex set of problems. You have to contend with every angle, from personal concerns to corporate politics — while putting firm controls on a fluid problem that can evolve and change right in front of your eyes. What appears ordinary and unimportant one minute can become a critical issue the next. The critical issue then becomes absolutely essential — and if the person in charge of slaying that dragon doesn't understand the process correctly, then suddenly your business could be . . . well . . . toast. All because *somebody* didn't take the time to read the memo or grab a copy of the plan or review a report on the BCDR process.

BCDR requires not only planning but versatility. It's not only a broad-spectrum approach to a critical problem, it also requires near-frightening attention to detail. It requires not only a conscientious overview of the problem, but an ability to tackle its

component parts — and the flexibility to understand how little things can cause big dollar losses. For example, consider how a failure to fund a series of backup servers (just because "there has never been a problem in the past") is asking for trouble. It's like failing to install fire extinguishers because somebody thinks they're ugly. (***Hint:*** Rubble is uglier.) But that sort of thinking is surprisingly common.

BCDR requires a serious and dedicated effort, not only to understand the problem (whether at the level of details or overview), but also to renew your company's comprehension and responses to a situation that's anything but stagnant and far from simple. Just as the problems that characterize BCDR are highly dynamic and forever changing, your business has to respond to ongoing change on an ongoing basis. Flexible and strong communications systems are invaluable when dealing with the dynamics of BCDR.


You cannot simply write the plan and then put it on the shelf. Paper that just sits there will still be sitting there when the gunk hits the fan. A BCDR plan, when done properly, is dynamic and complex. It's comprehensive as well as tightly focused. It's an ongoing work-in-progress with no clear beginning or end. When you undertake the challenge of BCDR, you will indeed be challenged. If you're going to be the white knight of BCDR, you can expect never to run out of dragons. Plan accordingly.

## More info from ASIS International

Since Business Continuity Disaster Recovery (BCDR) is a discipline closely related to security, ASIS International (Previously called The American Society for Industrial Security) can provide some very useful info. I have been a member of ASIS since 1975, and was part of a committee that designed and implemented a guideline publication that captures some of the essence of BCDR. I was one of the two primary writers of that publication (*Business Continuity Guideline — A Practical Approach for Emergency Preparedness, Crisis Management and Disaster Recovery*). It is available from ASIS International through their website — `www.ASISonline.org`.

# Keeping business continuity in focus

So what sorts of factors get in the way of effective BCDR? Well, it's easy to let the issues of business continuity get distorted by a lack of clear perspective. For instance . . .

## Staying calm amid terribleness and FUD

How big a problem do you really expect to have? How big is a "big" BCDR problem? Well, that depends partly on what your business is used to — but some problems happen on such a large scale that they affect *all* businesses. Between small and large are conceptual benchmarks beyond which we have difficulty — especially when we have to think beyond our comfort zone (say, when the numbers get too big to count on both hands). For example, consider a problem with a silly name and big teeth: the *Terribleness Factor.*

The Terribleness Factor is essentially a gut reaction that flaws the thinking process. (To get a handle on the nature of it, imagine a roomful of people running around screaming, *"This is terrible! Ack! Terrible!"*) It can set in just when what you really need is a clear thought process that understands the orders of magnitude of the problem — and what resources can realistically provide meaningful relief. It's an obstacle to effective action against whatever is so terrible. For example, Hurricane Katrina was way beyond what the world was prepared to deal with. But what worsened the disaster was a factor that goes by a rather silly name — FUD (Fear, Uncertainty, and Doubt) — in huge quantities. Understandably, emotions ran rampant in the face of compounded tragedy; everything not only worsened, but looked and smelled worse all the time — and made a well-thought-out, appropriate response nearly impossible.

## Real-world relevance gets buried

Most people habitually figure the real world is a pretty safe place (yeah, right), so they can't properly process the magnitude of disastrous events. As a result, their usual notions about what can be done to fix a bad situation are out of kilter. Usually they're thinking too small and acting too late or just not prepared.

Maybe the most efficient illustration is a stinky example: Suppose the neighbor's dog makes a mess on your doorstep right where it's highly visible. You have a fairly normal-scale problem. If every dog in the neighborhood comes to your door, you have a much bigger problem — but the average person's thinking might stop right there, as if the next logical response were to run around screaming, "This is terrible!" (Yep, that's the Terribleness Factor in action.) Then the local fertilizer company sends a dump truck to your door by mistake, and it dumps a truckload there instead of at the local farm. The problem suddenly leaps beyond terrible to inconceivable *("Now what do I do?" "Who's gonna clean this up?" "Who do I have to call or kill to get this cleaned up?"*) Then you see a whole fleet of dump trucks coming down the block: The brain freezes, unable to call the fertilizer company to report the mistake. Somebody call the Health Department.

### *Natural disasters as indicators of scale*

Natural disasters and so-called *acts of God* (check your property-insurance policy for the legalese) are clearly a larger-scale ugliness — hurricanes, tornadoes, earthquakes, tsunamis, typhoons, volcanic eruptions, sandstorms, mudslides, and tectonic plates shifting. (We'll leave the asteroid strikes aside for now.) Suddenly the whole environment seems to be out to get you. And if it happens again and again, suddenly what's "normal" starts to change.

So here's a thought: Since they ran out of hurricane names in 2005, it's a clear indication that we were unprepared for a real event — especially if you think of the entire hurricane season as one Big Event. That lack of preparation is denial in its purest form. Our current gauge of hurricane strength goes up to level 5, which is anything 155 miles per hour or more. Could we conceivably experience something worthy of a 6 or a 10? Maybe we need to set up a few more categories for hurricane strength, just to be in a position to understand a new scale of things — but that would only be a beginning, and how do you put that across when folks are still trying to dig out from (let alone understand) what happened to them? Guess what? This is a communications problem.

No surprise if many think the local police and fire department should have been able to help them better when Katrina struck. But the authorities were in no better position to protect themselves and their families than anybody else. The scale was too big, and there was no comprehensive plan that

everyone was prepared to carry out. Those who suggested that the victims could have been rescued by helicopters didn't really do the math. Again: too big an event, not planned and not practiced for, and no widely shared level of preparation.

### Human-caused disasters from out of left field

Human beings are nothing if not unpredictable — and manmade disasters illustrate how hard it is to predict where the next threat to your business will come from. The World Trade Center fell as the result of a human-conceived event that most of us couldn't conceive of before. Which was why it worked. Massive power outages — including cascade failures that involve entire states — only exist because of human technology. Weapons of mass destruction and other forms of military threat remain a plentiful source of disaster, whether real or potential (and that's not to mention their aggravation of the Terribleness Factor).

But it is our understanding of orders of magnitude that gives meaning to our thoughts. How can we tell whether we're thinking correctly or incorrectly about a potential problem? Do we have a realistic idea of what can happen, how likely it is, whether we can head it off, and how to recover from it? Well, some of us do, but . . .

## Who Do I Turn to for Expertise?

If the prospect of a frantic search for an expert, any expert, to help you with BCDR looks about as attractive as trying to pull teeth without a painkiller, take heart: You can start an effective BCDR plan with a little professional help in communications.

Avaya has addressed all manner of communications problems with creative solutions, outside-the-box thinking, and unique perspectives. They start with a simple — but powerful — idea: Almost nobody can master communications problems if they don't understand how the communications process works. That means understanding not only the technology, but also the nuances of business processes and the obstacles to correct thinking that can impede problem solving. Avaya has evolved the business of communications and problem solving to a fine art — as the following case study illustrates.


Just in case you miss it in the case study below, here's what may be the most profound statement in this entire book: *"The Avaya assessment has definitely given us control over the business that we didn't have before."*

## Case Study: Workers Compensation Fund

Avaya understands business continuity so well that other companies search them out for their collective wisdom. Workers Compensation Fund (WCF) is Utah's largest provider of workman's compensation coverage. "A prime contributor to WCF's success in the marketplace is the use of cutting edge applications and technology," says John Wallin, Assistant VP of Finance.

**Challenge**

Workers Compensation Fund has always been interested in business continuity, and though they had a good handle on it, they hadn't really approached it in a truly holistic or comprehensive way. Since WCF operates in a paperless environment, every core business process relies on imaged documents stored on their central mainframe and servers. WCF's list of high tech assets is impressive and includes a sophisticated imaging system, artificial intelligence, and self-learning neural network. This gives WCF great analytical and predictive power to be proactive in management of claims. They can readily focus whatever resources are needed and also use the system to fine tune policy rates. Technology is fundamental to the success of their business.

There is little room for down time in such a high tech environment. WCF understood the importance of business continuity planning, but it took the 9-11 tragedy to move efforts into high gear.

Avaya's Business Impact Analysis (BIA) was quite comprehensive and even extended to a review of physical infrastructure, including ways to improve fire suppression systems and enhancing the physical security of assets. Avaya Global Services also helped WCF get a better handle on the relative likelihood of different types of disasters.

**Solution**

Avaya ranked all of the critical business processes according to priority of restoration. This ranking was not by department, but by criticality to the overall WCF business. Each process received a Recovery Time Objective (RTO), the amount of time that the process could be down before the business suffered a significant impact.

WCF's databases received a similar Recovery Point Objective (RPO)

rating, which evaluated the acceptable amount of data that could be lost before restoration. As a result, WCF now has good insight as to what types of disasters are more likely to impact their business than others. This has allowed WCF to prioritize both their thinking and spending.

**Results**

- **False expectations exposed.** Avaya's observations were quite eye-opening, especially those showing that many existing recovery time perceptions were unrealistic. This was a real wake up call concerning potential business vulnerabilities. Another key impact showed who in the organization is in the best position to address these opportunities.
- **Improved assessment.** WCF performed a BIA (Business Impact Analysis) and it showed that the planning originally done for protection of information technology systems was pretty much on target. But those plans that were in place did not support the business processes that made use of them on an ongoing basis. Being able to restore a server is one thing. But when there is a batch of servers there are interdependencies and specific sequences that must be followed when bringing them back up. Which servers need to be fired up first? And then, which of them are tied to lines of business that are not really critical and can wait until later in the scheme of things?
- **Enhanced approach to solutions.** On their own at first, WCF took what appeared to be a logical approach and John Wallin himself was busy doing the research and writing the recovery plans for the various departments within the organization. WCF also invested in one of those software packages specifically designed for capturing disaster recovery information. WCF wanted to be sure that their approach was consistent across the organization and throughout the individual departments. It did not take long before it was evident that there was a significant amount of proprietary data, department specific information that only the department experts had and only they could manage. Before much longer, the routine daily operations were again foremost in everyone's mind and the importance of business continuity efforts was secondary. Their well conceived planning efforts all but came to a complete halt.
- **Avaya Global Services Professional Services.** The approach that Avaya used was team oriented and covered all of the bases. It spanned the entire WCF operation. The BIA (Business Impact Analysis) that Avaya did was comprehensive and took a hard look at both the technology and the functional processes and determined where there were strengths and weaknesses. The actual corporate deliverables

*(continued)*

*(continued)*

were identified and it was clarified how any interruption to either the operzating technology or the processes being carried out would adversely affect the corporate deliverables. Avaya carefully documented the deliverables and their specific vulnerabilities, and particularly as relates to critical business functions. They also documented the critical time frames, showing the maximum amount of time tolerable in each case before irreparable harm was done. This critical time information was captured along with information about what people were essential to the operation.

- **Inter-Relationships.** The dynamic relationships between normal operating procedures and the state of the art technology feeding into those operations was carefully investigated. There was also the question of how easily replaced is some of their technology. Is it something readily available or is it so unique that it is not replaceable except at extreme cost? And, how long would that take? The business of getting backup equipment and key people to the various recovery sites was another question. How long would that take and what would it cost? And how long could we do it before it didn't matter any more? As these and other questions arose and were answered, it became even clearer that the Avaya approach to identifying solutions to these problems was indeed the way to go. Avaya competency was unquestionable. And, through the process, Avaya provided motivation and encouragement to the staff to look at the whole recovery picture through new eyes that see it all and very clearly. Everyone that was part of the process feels that Avaya delivered a far superior evaluation than could have possibly been done without them.

*"Most fundamentally, though, Avaya has given us a Business Continuity process and baseline that forms the foundation of all our future efforts. The Avaya assessment has definitely given us control over the business that we didn't have before."*

*— John Wallin, Assistant Vice President, Workers Compensation Fund*

# Part II

# Developing Risk Management for Your Business

### *In This Part*

- Laying out the Risk Management Dependency Sequence
- Creating a continuity team
- Planning continuity operations
- Connecting with the communications angle
- Getting a closer look at a risk-management case study

So you think you may have a potential problem? What kind of risk are you facing? How can it be prevented? Answer those questions and you've taken a step toward risk management — and that's the first step in preventing a disaster (or at least keeping it from trashing your business).

Risk management is nothing new to managers who are used to enterprise-wide problem solving. What is new is the concept of *recovery* — actively preparing to bounce back from a disruption. Simply fixing things when they break is one way to look at recovery, but it doesn't begin to cover all the bases. To manage risk effectively, you have to strategize the deployment of resources — well before chaos strikes — for two reasons:

- If you're like most of us, those resources are anything but unlimited.
- The logistics of implementation — always complex — get difficult fast when business operations are disrupted.

Clearly, your best bet is to have a solid plan for getting things done — well before you're called on to do them. So far, so good. But what really needs to be done? You can determine the essential steps to take by analyzing what your business needs when it faces specific threats — and basing your risk-management strategy on that analysis.

## Heading Off Disaster Beforehand — Prevention, Deterrence, and Deflection

Prevention is security in action. *Security* is defined as the protection of life, property, and information. Basic prevention is a good thing.


One of the few tools that security has at its disposal is communications. Security is critically dependent upon phones and radios and television systems. Being able to maintain good communications in tough situations requires good planning, and lots of it. The technology available to us today disguised as a telephone is mind-boggling.

I will be discussing some of the tools of the security trade as I proceed through this text. But I want to make sure that I am clear on *deterrence* and *deflection.*

**Prevention:** You understand this one.

**Deterrence:** Nip it in the bud

**Deflection:** Fend it off or send it back where it came from. Send it next door.

Good risk management is grounded in realism, and that means taking bearings and applying common sense. Fortunately, the basic steps in the Risk Management Dependency Sequence are easy to list:

1. **Identify the risks:** Make a list of all possible attacks. Realistically, what can happen to your business or human life?

2. **Assess the risks:** Evaluate each potential risk. How likely are the ones you've listed? Okay, really how likely?
3. **Evaluate the risks:** Determine, in dollars and time, just how long you can go before the risk breaks the bank.
4. **Manage the risks:** Make preparations to manage and control the risks. That's where the effective use of resources comes in. But if you don't have good lists to work with, you are just guessing in the dark.

That's the sequence. The rest of the job is carefully filling in the details — so these next sections take a closer look at that process.

## Identifying all possible risks

A good risk-management scenario begins with a laundry list — of possible risks. Happily, compiling such a list is not rocket science. You can start by taking a critical look at local history and news media; a little common sense will tell you that tsunamis are not likely in the mountains of Tibet, blizzards are not likely in Hawaii, and volcanic eruptions are not likely in Chicago. But (for example) what about earthquakes? A little research into what's already happened will tell you what *can* happen. So far. That's a good first clue.

Some other risks that may find their way onto your list include fire, natural disaster, sabotage, power outage, loss of executive protection, loss of marketplace confidence, and so on. (Note that nature isn't the only source of trouble.)

When you have a reasonable list of possible incidents in hand, you can begin to rate them by how likely they are to occur.

## Assessing and evaluating potential risks

There are several ways to assess the potential risks that made it onto your "Most Unwanted" list. The approaches can be simple, complex, or somewhere in between:

- You can apply a simple subjective rating to each risk ("On a 1-to-10 scale, how likely do I think this is?") and compare the ratings.
- You can do a detailed what-if analysis, calculating specific costs you'd have to incur to cure each problem, and *then* rank the various incidents.


If you've had one of those grueling statistics courses that include calculating probabilities, put it to good use! Fortunately, there's rarely any need to get that fancy.

- Prepare a chart listing the potential risks, their likelihood of occurrence, and a severity rating for each one. Now you're getting somewhere — in this case, to a *BIA (Business Impact Analysis),* which is what such a chart is called. (***Hint:*** This is an incredibly useful tool.) BIA is covered in more detail in the next section.


Be sure to look at each item in your risk list as an individual potential impact with its own specific effects. Nuclear fallout (for example) isn't the same thing as an electrical fire, but if your business faces both risks, you have to understand accurately what each one is, what it does, and what specific problems it can cause for your business.

When you've got a good handle on the nature of each risk and how likely it is to occur, the next phase is to set up your risk-management procedures.

## Managing and controlling risks

Early in the risk-management game you must carefully take stock of your resources and review your potential for losing them. As part of losing them, you must perform what is called a *BIA,* or *Business Impact Analysis.* This detailed assessment of your assets and their importance to you is easily calculated. You give it a dollar amount of what it is worth. Then you determine how long we can live without it and how much you stand to lose for every minute, hour, and day you have to go without it. Each resource above a certain significant value must be considered. You use an *RTO* (Recovery Time Objective) to determine just how long you can survive without it . . . whatever *it* is.

In many businesses today it is their IT mission critical applications which make the case for business continuity planning.

Some applications relating to investments can lose millions of dollars in one day. With RTOs of only several hours and loss potentials in the six zero range, it is not hard to prioritize which ones are the most important to the organization.

# Developing Continuity Teams

*Continuity teams* are designed to make sure that the bad stuff does not happen. Bad stuff happens when certain things like critical resources are lost or fail. Communications, food, water, clothing, shelter, battery power, generator fuel, special paper, and special parts comprise critical resources. The risk of not having a critical resource as part of a recovery scenario is totally unacceptable.


Maintaining critical resources is important beyond all else. And it is the System Owner and/or Resource Owner who has the responsiblity to maintain the critical resource. A quick example of a critical resource is a vendor Web site. If the Web site is where all sales come from, every minute it is down costs money. People tend to behave badly when their money is affected adversely.

It sure would be nice if team development were a no-brainer — but it takes brains to organize brains. The thoughtful and successful development of teams is more difficult than many organizations realize. That's especially true of *continuity teams* — the folks who take on the responsibility of getting a business through disruptive incidents.

For one thing, maintaining continuity is practically a full-time job in itself. Well, okay, you can't expect to see a Department of Business Continuity crop up overnight in your company — but keep in mind that business continuity planning requires real commitment of budget, staff, time, and resources.


Many organizations fall into the trap of assigning the planning of a business continuity team to an already-busy employee — without providing any real support or budget. Unfortunately, just designating (or being) a good worker is not enough. If you plunk a Team Leader hat on someone who's already overcommitted, but leave out the means to perform due diligence, the result can be a very rude awakening.

## Assembling your team

Creating a continuity team means taking into consideration the special talents that your people possess, as well as the talents that your business absolutely must have in place if it's going to get out of trouble. When you set out to assemble your continuity team, you may already have one good tool in your arsenal — especially if your Human Resources department has created it — a *personal-skills inventory:* Periodically, all associates provide HR with a definition of their skills — an updated résumé, if you will.


Many people's skills increase dramatically over the time they work for an organization — in fact, many ultimately leave because their acquired skills go unnoticed. Handy as a personal-skills inventory is for planning special work details during normal operations, it's even better as a starting point for identifying who can help out the most in emergencies. (It's also a classic motivator, especially for people who enjoy a challenge and want to try out what they've learned.)


Whether you have a ready-made personal-skills inventory available from HR or create one specially, make sure your team has access to all the varieties of expertise it needs to keep running. One way to ensure that is to have at least one member from each of the following departments on your continuity team: HR, Information Technology, Facilities, Security, Legal, Communications/Media Relations, Manufacturing, Warehousing, Special Response teams, Engineering, Site Restoration, Payroll, Administrative Support, and Business Critical Support Functions. The members of the continuity team should all be under the clear direction of Senior Management or its representatives.

## Identifying roles using the classic management approach

Identifying roles in the plan is a simple management exercise. The individual roles must be built around written position descriptions. The responsibilities of the roles must address their duties. Executable duties must follow the classic management approach of planning, organizing, implementing, and controlling. Duties must be planned, organized, put in motion or implemented, and then carefully controlled.

# Establishing Continuity Plans

Making things happen in the middle of a disaster scenario is dragon-slaying at its best. But if you don't yet feel like a knight in shining armor, don't worry — help is at hand. The trick is to make use of it. If you are in charge of the continuity team for the company, it's not your responsibility to write the details of every department's plan. Not technically, anyway. That's the easy part. The much harder part is getting other folks to do it. Too often you may wind up trying to assign continuity tasks to someone who has no interest, no desire, no time, no motivation, no patience, no budget, no nothing. But fear not: This section will help you achieve just the plan you need.

## Getting the teamwork you need

Using the personal skills inventory is a good way to start your team building. Lacking that, you may see dragons waiting in the wings again. If you don't have the time or inclination to gather up all of the necessary people in-house to do this, you had best start looking outside. Companies like Avaya have done it all before and they can really surprise you with their knowledge and functional expertise.


When planning teams be sure to include all *critical areas.* Consider the impact of not including some specific area before you finalize your decisions. *Danger, danger* — whatever you do don't forget payroll! It's easy to overlook because it is not staring you right in the face at the outset. But, most people will not work long for free. And as a tactic, just plan to *duplicate the last payroll in the event of a disaster*. It will give HR and the payroll accounting folks some time to catch their breaths.

## Creating your plan

Some suggestions for doing this could be talking about the fact that this is going to involve a lot of writing and assembling documentation. (This is very tedious for some people — some people just plain can't stand it.) Commiserate with them, and then suggest that writing a little bit each day or assembling a little bit each day will make it less painful. Most people are not so disciplined. And — if it is just too painful they can always *outsource* it to a vendor . . . ah . . . like Avaya.

Take an accurate organization chart and identify must-haves and everything else as two separate groups. Once you have the two separate groups, apply *RTO* (Recovery Time Objective) ratings to the must-haves. Then design the plan from the standpoint of *NO ACCESS TO THE BUILDING!*

And, I'm telling you, don't forget payroll!

# Communications and Continuity

Communications fits into the overall equation of business continuity in so many places that you might as well call it the glue — or the lifeblood — of the equation. How so?

## Securing your communications

Securing your communications facilities and all attendant resources is usually a very good thing to do. Telephone and IP system servers should be kept behind locked doors, properly air conditioned and properly backed up. Power systems should also be backed up with a UPS (UPS stands for Uninterruptable Power Supply — it has nothing to do with anything brown). When it comes to UPS systems, check out electrical contractors and engineering companies. UPS is more of a facilities and building engineering concern.

You should always take advantage of the multiple capabilities available to organizations in communications. There are many strategies that an organization can use to strengthen and protect their communications infrastructure to make it resilient to disruptions and crises. A few that come to mind are creating diverse communication paths of many kinds, identifying single points of failure in the call path, implementing an emergency notification system, and identifying their best options for communicating during an emergency, whether it be land lines, VoIP, radio, satellite, wireless, or cellular. If you really want to get creative, you could even consider something like a runner or the Pony Express. Getting budget approved for the animals might be a bit of a stretch. Just kidding, of course.

## Managed services operations

There are many options for companies to consider as they explore business continuity strategies and develop their plans. One option to consider is to outsource the company's critical communications functions that impact every relevant portion of your business, partners, and the customers you serve. Would you consider cutting a deal with one of your competitors to subcontract services to you under a nondisclosure, restricted non-compete clause to lend you a helping hand in your time of need and vice versa? If that idea is too radical, explore service providers or communications companies, like Avaya, who offer a range of managed and hosted services options, along with providing emergency network units that can be shipped to disaster sites.

Managed services operations are fully functional centers providing wide-scale support across communications and applications. Consider companies who have service centers located throughout major metropolitan locations in the world. Ask how they will keep your records secure, what technologies they can support, how easy (or difficult) it is to turn your systems back over or take them over in the event you need to act quickly. Imagine developing a strategy that didn't consider the impact of a centralized contact center operation, the physical re-location of your workforce and ability to keep your business running even if the campus doesn't exist.

Don't forget about Avaya maintenance when things are going horribly wrong. You know that Avaya will be there for you twenty-four hours a day, seven days a week, 365 days a year.

## Using VoIP to best advantage

Ma Bell is truly a thing of the past — and that's just as well, given the high speed and high volume of data needed for doing business. Increasingly, twenty-first-century business communications uses *Voice over Internet Protocol (VoIP)* — a relatively new technology that uses the Internet instead of normal PSTN (Public Switched Telephone Network). This new twist in the telephone world has offered a way to dodge overloaded or crashed phone systems and otherwise undependable conventional phone systems.

VoIP provides a ready alternative to Ma Bell. VoIP users can plug in anywhere there is an internet connection and carry their personal number with them. Sounds fantastic, doesn't it?

You will soon be saying, "Can you hear me now?"

Here's a typical case study that illustrates how VoIP can make a crucial difference in keeping a vital organization up and running. Note especially how applying sophisticated telephony can make the system more reliable and enhance business continuity.

## Visiting Nurse Service Relies on Avaya IP Telephony to Deliver Vital Healthcare Services across the Big Apple

With a mission to provide vital home healthcare services to a population of more than 10 million, Visiting Nurse Service (VNS) of New York has a very big responsibility. Each day this 110-year-old non-profit organization dispatches some 5,000 clinicians, therapists and home health aides to provide a wide variety of in-home services, including senior and private care, after-hospital and rehabilitation therapy, hospice care, children's and family services, and more.

In all, the VNS staff of 7,800, located in nine major locations and in hospitals across the area, makes more than two million visits to some 100,000 clients each year across Nassau and Westchester Counties and the five boroughs of New York. For more information, visit `www.vnsny.org`.

**Challenge**

VNS continually seeks to improve and enhance its delivery of client services. VNS believed that new communications solutions coming on the market could significantly improve the organization's performance and provide the foundation for future gains, and was eager to take advantage.

A major area for continuous improvement especially important for VNS is business continuity. Because VNS provides a healthcare lifeline for thousands of shut-in clients, to be out of reach is simply out of the question.

In terms of business continuity, there were times when data network problems knocked regional VNS offices offline and shut off the essential flow

of clinical, human resources, and financial information. A series of events, including virus attacks, a neighborhood power outage in 2001 that affected a major VNS site in Manhattan, and the September 11 terrorist attacks in New York, brought home the need to strengthen the organization's communication continuity and capabilities.

Another area for enhancement was identified in the VNS contact center and the supporting CENTREX system. The organization believed newer technology could deliver enhanced contact center capabilities. VNS also realized that a new system would offer opportunities for greater efficiencies based on easier administration.

**Solution**

VNS chose the Avaya IP Telephony Solution as a strategic platform for keeping VNS on the cutting edge in providing superior client service. The Avaya intelligent communications solution ensures business continuity and continuous communication across the Metropolitan Area Network, creating an "always on" communications environment to support mobile workers and clients utilizing the latest unified communications and mobility applications.

**Results**

- **System reliability and business continuity.** Even if a VNS site became inaccessible, the client service staff could easily continue their work from another VNS location, or even from home. Redundant servers at the two main Manhattan locations provide reassurance that VNS professionals will be available for their clients. A more robust network virtually eliminated frame relay problems and cut voice communication problems to zero.
- **More personalized customer interactions and faster service.** In the contact centers, call distribution based on agent skills now helps callers reach the right agent faster. Seeing that they could deliver more personalized customer service by funneling calls to their groups through the Avaya Call Management System, contact center managers expanded capacity: The Avaya Call Management System now serves some 250 agents, up from the maximum of 100 possible before the Avaya solution. When clients call their regional offices after hours, they are automatically transferred to the main contact center.
- **Improved contact center management.** Contact center managers have the ability to gather and analyze contact center performance statistics. Before, answering questions about such key issues as call volumes or speed of answer required an educated guess.

*(continued)*

*(continued)*

- **Enhanced mobility provides increased responsiveness.** Avaya Modular Messaging delivers voice messages, fax, and e-mail to over 1,000 employees over their PCs or their telephones, making it easier and faster to check and manage messages, and users can respond faster and work more effectively from any location. VNS call center agents can also work from anywhere using laptops equipped with Avaya IP Agent software and simply logging in to the Avaya Media Server. For a select group of VNS staffers, who must be quickly available in any circumstance, Avaya Extension to Cellular instantly bridges office calls to their cellular phones. Callers no longer have to carry and dial a laundry list of reach numbers to make contact.
- **Reduced costs and improved staff productivity.** Moves, adds, and changes, which previously required precious staff resources and often took up to a month to complete, are quick and easy due to the straightforward administration of IP endpoints. Another huge payoff for VNS: a net savings of $900,000 yearly in communications expenses. Five-digit dialing now links all locations, and faster linkage of people and processes fosters more productive collaboration.

# Part III

# Implementing Your BCP (Business Continuity Plan)

### In This Part

- Planning and organizing the procedures
- Implementing the nuts and bolts
- Controlling the processes
- Checking out a real-world case study

Bringing realistic solutions to business-continuity problems isn't all that different from solving any other type of business problem. The four tenets of management — Planning, Organizing, Implementing, and Controlling — are center stage. Some people like to think in terms of Readiness, Plan, and Practice. This is equally accurate. After 9/11, New York Mayor Rudy Giuliani toured the United States touting the message of Readiness, Plan, and Practice.

This chapter addresses each of those tenets in turn, regardless of what you call them, and shows how communications issues are at the heart of each one. The logic of using business management to approach business continuity is clearest when you think about communications as the sharpest, most flexible (in fact, best) tool in the shed — and sometimes the only tool that gets the job done.

Ask any mechanic and you'll hear, "There's nothing like having the right tool for the job." But beware! Having the right tool doesn't mean it's a no-brainer to use.


Business-continuity communications can get you into trouble in a heartbeat if you're not careful. Being "creative" in your approach to the whole shebang — Business Continuity and Disaster Recovery (BCDR) — is fine as long as you hit your target with just the right amount of force. If what you need is a hammer for your BCDR nail, you may not want to swing a ten-pound sledge at it, any more than you'd want to swing a coffee mug. There are so many wrong ways to do it. How do you find the right one? Three word answer: Practice mock drills.

Fortunately, the classic stages of management — Planning, Organizing, Implementing, and Controlling (or Readiness, Plan, and Practice) — are a natural progression. As you follow that progression from early thoughts to final products and ongoing maintenance, think about the need to keep the process healthy.


POIC done right avoids FUBAR. Translated from acronym-buzz, this means: Watch your step at every stage of Planning, Organizing, Implementing, and Controlling (POIC) your communications techniques and tools. Sloppy planning and lack of proper focus can (ahem) foul things up beyond all recognition (FUBAR).

# Planning and Organizing

The thoughtful planning and organizing of business continuity is (luckily) an area in which Avaya excels. Its approach to communications consulting helps clients pinpoint problems and then (ten-hut!) perform a surgical strike without collateral damage. The results often spur overall improvements in business procedures that go far beyond the original intentions. (Clarity and efficiency — what a concept.)

## Planning

As with any major business process, planning means getting a firm handle on the flow of information. That's especially true of communications; we must be able to gather up all the information we need — both at the outset and when the unexpected lands in our lap — to manage our way through a disaster scenario.

Starting from Square One, the most important tool for gathering the needed information is your BIA — Business Impact Analysis. The process of creating one gives you a consistent picture of what parts of your business would be impacted the most by a disaster. The challenge is then to focus your problem solving skills in those areas and identify good communications solutions.

The BIA identifies and helps expose the vulnerabilities that will be the most sensitive targets in a disaster. Chief among the weapons to use against the *dragons of disaster* (sounds like a rock band, doesn't it?) are your communications resources.

## What is a communications resource?

Here I'm talking about any aspect of a system that contributes clarity and efficiency to the process of communications. Also, a communications resource can be many kinds of endpoints — radio, satellite, ISDN, cellular, wireless, IP analog or digital phone, etc. A company wants to consider the options they have in communications resources — then choose what is best for their situation. The average company needs to have the technology presented to them by talking about how diverse the options are and how they can choose what works best for them. Those who don't have a clue about the technology simply have to hire someone to hold their hand through the process. A perfect example of the technology is Avaya's SIP (Session Initiation Protocol) — a protocol used for VoIP. It is a way of getting lots of different devices to trade information efficiently. Avaya SIP integrates multiple devices that users handle — say, cell phone, desk phone, PC, PDA, customers, and vendors — seamlessly. Quite aside from the increased efficiency and productivity that results naturally from such integration, imagine how that integrated system can help get your business through a crisis. (***Hint:*** Less confusion.)


Avaya uses system integration as a catalyst for the next phase: open communications over the Internet (using, of course, heavy-duty encryption and Internet Protocol). SIP is an interoperable protocol; you can use it to connect products from multiple vendors, which creates new possibilities for system flexibility. That's especially handy for multi-service

networks. Organizations can make best-of-breed picks from a variety of vendors to create a seamless, converged communications network.

Here's an instant advantage: As a growing number of enterprise leaders consider organization-wide migration to converged communications — VoIP in particular — most test the waters one application at a time. Do baby steps first. Initially, the savings anticipated from VoIP include improved business continuity, bypassing phone-company tolls, and ease of administration when the business had to grapple with moves, additions to the system, and other such changes. These days, the increased flexibility that VoIP offers for deploying new capabilities and integrating applications makes migration to converged communications even more attractive in a wide range of enterprise environments.

So, what is SIP other than a VoIP protocol? SIP is different from proprietary communications protocols because it enjoys wide industry support. What you get is a practical means of integrating multi-vendor equipment at the highest level of the protocol stack — the Application layer of the OSI Networking Model. OSI is Open Systems Interconnection and relates to the seven layers of network connection. The OSI Reference model speaks to the seven layers, describing how various applications can run on the same network-aware devices and still communicate with each other effectively. This is the beauty of interconnectivity. Just plug it in and go: radio, satellite, ISDN, cellular, wireless, analog or digital phone, computer, printer, fax, copier, hard drive backup, PDA, photo printer, game system, kitchen sink, and shoe shine box. People now carry flash drives and PDAs instead of legal pads.

## Converged communications

So what's this converged communications thing got to offer and where can I get a lot of it fast? Okay, first things first: *Converged communications* means getting just about any technology to talk to any other technology. The ultimate convergence and the ultimate evolution are the same: When everything talks to everything else, you can put information wherever you want it — and use the same system to manage your way out of a disaster — all using the existing infrastructure of the Internet, while maintaining security.

Bottom line: Barring an asteroid strike or other global endgame, there need be no such thing as a "total" disaster.

Convergence is going on as we speak, and our devices depend more and more on it. Take, for example, the current generation of computers; they're designed to be hooked up to all sorts of other devices. Just plug it in and it talks to the new hardware.

These days you can build a business continuity scenario that uses — consistently and efficiently — many different devices. That means you have a wider range of capabilities you can draw upon to manage the hairy communications traffic of a disaster scenario. Even in the course of everyday business, you may wind up working with a client in the car who communicates using a cell phone, a laptop with wireless capabilities, a PDA with wireless and Bluetooth capabilities, or all of those. (Speaking of disasters, let's just hope somebody else is doing the driving.)

Clients who happen to be near offsite computer connections can tie in to various VoIP systems and conduct critical conversations when normal phones (PSTN — Public Switched Telephone Networks) have gone belly up. For that matter, so can members of your disaster-management team.

## Organizing

Actually organizing the details of business continuity means scrutinizing your Business Impact Analysis and using what it tells you as a guide for your next steps. When you've identified your communications resources and used the BIA to pinpoint where they need strengthening (or are already pretty good), you have the basis for a business continuity roadmap to work your way through the problems you've so carefully identified. With a clear picture of the possible losses in lives and dollars, you can target just where to apply communications solutions to reduce those losses.

Organizing your business continuity approach means

- Lining up the data you've gathered and turning it into lists
- Assigning ranks to both the potential problems and their solutions

- Evaluating the effectiveness of the resources you have in place
- Positioning your resources where they can do the best job in the shortest amount of time


Any Business Impact Analysis that's worth its salt communicates the dreaded Recovery Time Objective (RTO): that scary figure that tells you how long (at best guess unless you tested it!!!) it'll take you to get back up and running. Using communications resources and interconnectivity provided by new technology and intelligent call center software can get you to your RTO as quickly as possible by making the communications flow quickly and accurately.

# Implementing

As always, talk is cheap. Actually implementing your solution and deploying those resources all over your business's problems . . . well . . . that's where we separate the knights from the squires. The Business Impact Analysis serves as a map of the dragon's territory. The dragon-slaying sword puts the communications tools at your disposal such as SIP, or an intuitive call center. But there's no point in just coming out swinging willy-nilly; what's needed is a carefully coordinated attack. In some areas, the dragons will back off after only a show of force; in other areas, the battle will be vicious and bloody. Don't be surprised if, say, those computer-illiterate executives who block or deny the business continuity process get consumed in the heat of battle — or end up gibbering, "There was only supposed to be *one* dragon; they ganged up. No fair!"

Given that the telephone is usually the system that most companies want to recover in the event of a disaster (and never want to lose in the first place), check the armory.

- Today, an Internet based telephony backup is a very good choice. Tomorrow, who knows? Call Avaya!
- Intelligent Communications call center software means there's always a faithful messenger able to get the word out.

Being able to communicate effectively during an unfortunate incident (that you, of course, are well prepared for) says that you had an *incident* — but not necessarily a disaster.

Even so, the implementation phase is also the point at which somebody has to make a decision and *declare* an emergency if there is one. The actual declaration of an emergency is a big thing. You don't want to yell "Fire!" in a crowded castle. On the other hand, if it flies like a dragon, scorches like a dragon, eats the livestock . . . could it be . . . ?

## Declaring a disaster

The actual declaration of a disaster or other emergency requires a well-planned communications campaign. Someone who has the proper authority to declare that *we are officially having a disaster and we are invoking our disaster plan* has to set the wheels in motion by communicating — firmly and calmly, over all the appropriate channels — that the gunk has hit the fan. It helps if that person is *prepared* to do so. Practice makes perfect!

Declaration is expensive. Hotsite usage starts up, costing thousands of dollars per hour. People get dragged out of bed on the other side of the planet and their language is unprintable. Critical databases and security protocols go into action, moving massive amounts of data, making major shifts in operations, digging in to make ends meet while the situation's going on.

When it's time to declare, the declaration order must be communicated fast and authenticated — over a very wide area quickly. Here are some quick pointers:

- Call trees are best for critical staff. Cell phone and PDA notification works well here. If there is a complete communications loss like with 9/11, a common meeting place can work. If others are within walkie-talkie distance, grab the unit, chargers, and spare batteries and go.
- Preplanned corporate communications and media responses work especially well, and some of those can go up on the company Web site if necessary.
- Satellite phones are good as long as they are not dependent on land bound protocol and control.
- A canned message can go a long way toward satisfying the media as the executives catch their breath and plan the next response after the initial incident and (okay, let's be optimistic) successful first response.

# Controlling

Controlling the flow of information during an intense situation requires that you maintain open lines of communication and stay on top of operations as they're progressing. Keeping your phone lines open is where Avaya's intelligent communications call center software and flexible Internet Protocol solutions come into their own. They can be the first step in downgrading a disaster to an "unfortunate incident."

The staff can still make and receive calls on all their normal numbers. Customers can still access all your representatives, even though you told them to stay home and work in their bedroom bunny slippers. (They love that! And it helps improve the emotional situation.)

Everything keeps running smoothly and seamlessly to those who need it most — even if the facilities director, the security director, and the maintenance superintendent look like they've been mud-wrestling. Seamless operations maintain customer confidence.

The Controlling phase also means picking up the BIA again to look at the numbers. It also means having all your ducks (or at least team members) in a row long beforehand. Every critical resource must have an owner who is responsible for the maintenance and upkeep of that resource. In concert with that resource there must be a clearly communicated RTO (Recovery Time Objective) that specifies the amount of time you have to slay the problem before the dragons get loose or the dogs run away, whichever is worse.

If (for example) an investment house stands to lose a million dollars every hour that their phones are down, then they'd better make sure their phones don't go down. If they can lose *ten times that* if their Web site goes down — and it's vulnerable because it's only shown on one server — then the dunderhead who decided to not purchase a backup server will probably either get fired or taken out into the yard and offered to the dragon (same difference). If the phone system goes down and the Avaya backup system picks up the load without so much as a hiccup, everyone is happy.

## Approaches to testing

Testing is part of the Controlling phase of the process. The best approach to testing depends on three factors:

- The relative maturity of the organization (how long they've been in business, not necessarily whether they skateboard to work)
- The organization's ability to respond to events with appropriate measures
- How well the organization understands what's happening when it happens

That last one's tricky. Understanding what is happening when it happens requires lightning-fast communications. Responses can range from a security guard at a desk in the middle of the night calling the boss to start the ball rolling toward an actual declaration or — sometimes — an automatic electronic signal from an alarm panel.


If various levels of disaster can jump your business, you have to determine as many as you can and devise an appropriate level of testing for every one. And don't forget that they can occur in combinations like they did with Katrina. Phone systems were down, floods incapacitating everything beyond normal emergency supplies (hospital emergency generators ran out of fuel), massive numbers of people beyond what anybody was expecting who then all decided it was time to leave, and the list goes on and on. You need to be able to take the what-if scenario into the Terribleness Factor realm.


Take a moment and think about the teacher who gave a test that was so hard that the whole class flunked. A test that's overly harsh and makes everyone look bad is (in practical terms) universally politically incorrect. It can cost people their jobs. It may give some folks a reason to join ranks with the dragons and come back after you if you put them through an unmerciful exercise. What you want to do is to show them what can happen and how to come through it.

Testing and practice should be well planned in advance — and its specific parameters agreed to in advance. Here's an example:

A major earthquake damages the building and makes it unusable for the foreseeable future. Avaya communications backups using SIP protocol can provide replacement desktop architecture not only on a computer located someplace else, but it can bring up the same screens on a PDA or a virtual private network anywhere in the world.

## Techniques for testing and practicing

Time to grab that trusty Business Impact Analysis and make lists of areas to test. These should represent your communications systems, your computers, your servers, your client-based servers, and any other resources and systems you deem critical.

Then you decide how much detail to get into, and what level of test to perform. The short list of tests looks like this:

**BIA:** Always start off with a good BIA.

**Bench test:** This is an orientation walk-through (Baby Steps) that introduces your team to the outline of the problem. Often it is no more than a discussion and clarification of the call tree.

**Bench test:** This tabletop exercise can go into a bit more detail (Big Girl/Boy Steps) and takes the team through a complete description of an emergency and a response. The call tree may actually get called to see if it works.

**Applications and procedures evaluation:** Here's where you get the lowdown on the credibility of your business continuity plan so far.

**Simulation drill:** Put the crew through their real-world paces.

**Planned and announced test versus surprise test:** Use both; each is educational in its own way. From a preparedness standpoint, of course, surprise testing is the ultimate testing format.

Audit-department testing is also a worthwhile way to test a business continuity plan. The Audit Department can devise tests for your communications systems that you would probably never consider. They can present aspects of communication that are important to other areas of the company — for example, where recovery has to happen within 3 or 4 *hours* when you might normally feel comfortable with 2 or 3 *days*. Yikes!

Recovery-time objectives are the business continuity equivalent of Beat the Clock. Get everybody to shoot for the lowest possible RTO that gets the job done while keeping cost and human life impact top of mind.

With backup systems designed to support automatic switching and database sharing, RTOs can be kept low without breaking the budget.

## Avaya Global Services — Helping San Francisco International Airport Ensure the Highest Levels of Emergency Preparedness

As one of the busiest airports in the United States, San Francisco International Airport (SFO) has continued to thrive over a 75-year history, expanding from a staff of sixteen with fewer than 5,000 travelers in the first year of operation, to a current staff of 30,000 and annual passenger counts of more than 32 million.

**Challenge**

Those who depend on the airport comprise three basic groups. They are travelers of course, airline and tenant personnel, and the Transportation Security Administration (TSA). Each of these groups has its own special needs. But, the one overwhelming need that is common to them all is the need for dependable communications, and that it be up and running at all times. Travelers are becoming more specific about their needs. They want speed of service, comfort, wireless network access, and good cell phone signals. If they can't get these at San Francisco airport, there are two other airports that are close enough to offer serious competition. Most people wouldn't think that airports actually have to compete for customers. In 2003, SFO was named the Most Tech-Friendly Airport in America by

*(continued)*

*(continued)*

the Consumer Electronics Association in their annual passenger survey.

**Solution**

With information technology functioning like a profit center and with airport personnel and travelers all looking to keep expenses down, a new standard benchmark is developing concerning the so-called really good airport. The airport is now looked at as a business and not just a location to travel to and from. The communications systems and supporting infrastructure also demand that all communications systems be up and on at all times.

With this in mind, business continuity and other aspects of emergency preparedness become key issues. Knowing that to guarantee a level of service on an ongoing basis was going to require a consummate expert in the communications field, SFO chose Avaya. This all started several years earlier when Avaya was chosen to provide a new phone system.

Avaya evaluated the total network picture and the full communications package that would be required to support airlines, police, travelers, and concessionaires and their network needs.

Avaya has shown themselves to be the perfect Services Team. Spot on Project Managers and wizards for technicians make for ongoing success stories and minimal downtime.

**Results**

- **Avaya conducted Business Continuity Assessments in two primary areas, namely SFO network systems, and then they did an assessment of security systems.** Both assessments were very methodically done, leaving no stone unturned.
- **SFO received a detailed inventory of all of their complex equipment, including an assessment of the wires and how they were run.** Once an understanding was gained of what there was physically, Avaya launched into their business continuity evaluations of what was really vulnerable and they ranked everything that was critical for survival as a world-class airport. The Avaya assessments were so highly detailed, they ended up identifying every piece of equipment in every cabinet and ranking it.
- **It became clear that the technology that was supporting critical business functions and core businesses needed to be better understood in terms of what is really important and what is not.**
- **Nobody in the airport had ever seen a set of reports like the ones that Avaya handed to the airport management.** The reports were comprehensive, detail oriented, and showed the critical relationships between the

various equipment and the service SFO is required to perform. The quality of Avaya's work was beyond reproach.

- **All critical systems that support and maintain business continuity were evaluated and their relevance documented.**
- **Airport management reported that the Avaya Business Continuity and System Security Assessments provided a look into SFO operations that now allows them to better prioritize expenditures and investments.** This increased understanding of the operations from the ground up is something that is characteristic when it comes to Avaya.

Learning and understanding what to do about emergency situations makes the other stuff fall into place that much easier.

# Part IV

# Top Ten Reasons to Develop a Business Continuity Plan

### In This Part

- Complying with Sarbanes-Oxley
- Meeting federal laws and mandates
- Recognizing international disaster activities
- Enhancing processes and planning
- Preserving and improving application availability
- Avoiding and recovering from a disaster
- Having the power to save lives as well as your business
- Saving money by saving data
- Ensuring your company's future
- Taking control of your business operations
- Increasing your profits

Business continuity needs to be a part of your daily routine in your business. The reason is the clear logic of business continuity escapes many people who settle into an organizational niche and then just blunder on and on, totally oblivious to the obvious, entrenched in perfect denial ("hey, nothing has happened *yet*"). And then the two-by-four falls — followed by a ton of bricks. So here, as a public service to those of you who have undertaken to (ahem) *enhance the motivation* of those who are still in denial, we present ten good reasons to develop a business continuity plan. (Okay, so there are more than ten — consider the extra ones freebies.)


Continuing business operations is the core focus of any business continuity plan, and without good communications, all plans are prone to failure, delays, loss of revenue, placing people at risk, and the list continues.

## Sarbanes-Oxley Compliance

In 2002, in the wake of some hugely famous corporate scandals — think *Enron* (and then think *man-made disaster*) — the federal Sarbanes-Oxley Act went into effect. It sets especially high standards for accuracy and reliability in the corporate disclosures of companies that have a financial responsibility to their client investors. For openers, it specifies that the records that substantiate the financial position of an organization must be protected, maintained, and kept available. Think *major system crash* and *major lawsuit* (and then think *man-made disaster*); a word to the wise should suffice.

## Complying with Federal Laws and Mandates

Okay, suppose you're working up a business continuity plan for a financial institution and you want to make sure it's squared with the feds. Who do you call? Answer: the Federal Financial Institutions Examination Council (FFIEC). It's a formal body that's connected to various government agencies, and it's empowered to prescribe the uniform principles, standards, and report forms used in the federal examination of financial institutions. The agencies that do the examining include the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS). In addition to providing those agencies with the means to make consistent investigations, the FFIEC can make recommendations to promote uniform supervision of financial institutions. It's one among various federal watchdog organizations that keep tabs on the flow of dollars — and on the procedures that govern the flow.

HIPAA is the U.S. Health Insurance Portability and Accountability Act of 1996. It requires the U.S. Department of Health and Human Services to establish national standards for electronic healthcare transactions. It also looks to improve the security and privacy of health data by encouraging the widespread use of controls relating to electronic data interchange in healthcare.

GLBA is the U.S. Financial Modernization Act of 1999, also known as the "Gramm-Leach-Bliley Act" or GLB Act. This legislation includes provisions to protect consumers' personal financial information held by financial institutions.

## Acknowledging International Disaster Activities

The international groundswell in this area is incredible. Norway has developed a tsunami warning system. Hawaii is the center for much of the disaster reporting in the Pacific Ocean. Thailand and India are in a joint effort to produce a *world class* tsunami warning system by 2007. China is looking to revamp their disaster warning system and is seeking international cooperation. Disaster Prevention Law and Policy is one of the most urgent tasks facing the Chinese ministry. Indonesia is working with German scientists to develop a system.

Salvano Briceno is Director of United Nations International Strategy for Disaster Reduction and is proposing a World Wide Disaster Warning System, saying that we need to get everyone on the same track.

The British government is proposing a Global Disaster Warning System.

And all of this activity is just the tip of the iceberg. Bad pun.

## Improving Functional Processes and Streamlining Operational Planning

Audit departments love this part. They get to evaluate systems and procedures, scrutinize corporate efficiency and accuracy, and save money. The good news is that you can help them do that. Strategic planning gets easier and more effective when a good BIA (Business Impact Analysis) lays out what should be done to handle — and protect — corporate resources more effectively. Streamlined approaches to resource management and contingency planning are a natural result when organizations take BCDR issues seriously.

## Maintaining and Enhancing Application Availability

If a computer application is critical to the operation — say, when the company can lose over a million dollars per day (or per hour) when the system is down — then heading off that disruption should be a high enough priority to get the attention of higher-ups without much fuss. But if they're reluctant to talk about Business Continuity Disaster Recovery openly and honestly, you'd be well advised to document their position on the issue (to protect yourself in case that ton of bricks *does* fall on the system). Then let responsible management know (tactfully, of course) about the problem. This can be one of those dangerous situations in which organizational influence overrules common sense — and the ones responsible for keeping everything running are put at risk.


But if nobody says anything, just remind them that the business is at risk when uptime goes south.

## Disaster Avoidance and Recovery

Having a business continuity plan on record when bad things happen means the organization has a keen clue about what to do — and has the opportunity to prepare for impact, gather resources to thwart the problem, and (given a good plan and a little luck) stand back and watch the problem go by. To Detect, Deter, and Deflect is the initial sequence that leads to a successful recovery scenario. Hopefully, Defend can sit on the sidelines. Good communications systems go a long way toward enhancing preparedness — and (as a side benefit) just making the business run better.

## Saving Lives with Disaster Prevention

We don't really have to *argue* about saving lives, do we? Okay, maybe not quite everybody believes that there's more to life than business, but maybe they haven't thought it through: After all, you have to *be* alive — and have live customers — if you're going to do business with anybody. For that matter, if you can deflect a threat to life by preventing a disaster, your organization and the community are always better positioned than they'd be if they had to *recover* from one. (The beauty of prevention is like efficiency in the kitchen: If you don't make a big mess while you're fixing a big meal, you won't have a big mess to clean up.) If you're well prepared, you can Detect, Deter, Deflect and Defend — to keep both your people and your business alive and kicking. And here again, it is the Terribleness Factor that makes accurate detection a major problem. Knowing that you have a serious problem is far different from thinking you might have a problem. Being able to Detect, Deter, Deflect and Defend are part of the non-sugar-coated real world of corporate security, business continuity and protective services.

## High Cost of Lost Data

Think of data as the lifeblood of business. Data loss is as critical to an enterprise as blood loss is to a body. Given that perfect protection is not possible — but effective protection is — how much you're willing to do to protect your data becomes a simple business analysis of risks. A good Business Impact Analysis will show the risk of loss in revenue, spread out over some specific time window. Typically such an assessment looks at such costs as backing up, storing, and transporting data to wherever you need it — as well as how much it costs your company (per minute, hour, day, week, or longer) *not* to have acess to data as required. Some organizations will increase their risk — surprisingly quickly — for want of some critical data resource.

## Keeping Your Company in Business

If your business expects to be around for the long haul, then it is a really good idea to develop a business continuity plan. All the potential hazards associated with not having a plan will still be there whether you develop a plan or not — but imagine being in the position of saving the company *before it needs saving.* With a proper BCP (Business Continuity Plan) designed from the learning from a good BIA (Business Impact Analysis) your ability to Detect, Deter, Deflect, and Defend are all greatly enhanced. Otherwise, send in the dragons.

## Getting a Better Handle on Business Operations

Preparing a BIA shows where there are strengths and weaknesses in your organization's daily processes. Business operations can be running along for decades with little change — and then suddenly face a need to restructure around a less expensive way to make their product or a less expensive way to transport it. For example, most companies realized in the 1990s that sending a ten-pound manuscript by US Postal Service or

overnight courier to the other side of the world was more expensive than sending an e-mail with one or more attachments. (Don't be surprised if your business gets similar wake-up calls from time to time as technology evolves.) For many organizations, the BIA triggers reasons for dynamic and ongoing change. The organization's newly found ability to identify and properly address performance issues — and better control the costs associated with resource management — becomes (after business continuity) nearly their sole purpose in life.

## Saving Money and Improving Profits

Better management of corporate resources will always save money and improve the corporate bottom line, as surely as turning off a light switch will save the company operating expense. Being able to shift quickly into an effectively preventive defense is an advantage, especially when the adversary is still expecting you to fail at any minute. Surprise is something that most people hate — and good planning removes (or at least substantially reduces) the element of surprise — which puts your business in a better position to stay prepared and ready.

# Glossary and Acronyms

Some of the terms that describe business continuity are actual English words (sometimes used in new ways); others are the alphabet soup of biz-buzz and tech-speak. Here's a starter list of both species.

## Glossary

Here's the part of the business continuity vocabulary that reads more or less like English.

**alternate worksite:** A designated work location, other than the primary location, to be used when the primary location is not accessible.

**business continuity:** In effect, being prepared to run your business no matter what. Reaching that goal means a comprehensive, managed effort to prioritize key business processes, identify significant threats to normal operation, and plan mitigation strategies to ensure effective and efficient organizational response to the challenges that surface during and after a crisis.

**Business Continuity Disaster Recovery (BCDR):** This is the whole kit and caboodle of procedures, disciplines, and systems that ensure the ongoing preservation of acceptable business operations while preserving the integrity of corporate systems.

**Business Continuity Plan (BCP):** An ongoing, structured process — supported by senior management and specifically funded — to ensure the performance of three overall tasks: identify the impact of potential losses, maintain viable recovery strategies and plans, and ensure the continuity of operations (through personnel training, plan testing, and maintenance).

**Business Impact Analysis (BIA):** A management-level financial analysis that identifies the impacts of losing an organization's

resources. The analysis measures the effect of immediate resource loss — and of escalating losses over time — to provide reliable data upon which to base the decisions that will guide mitigation, recovery, and business continuity strategies.

**coldsite:** A predetermined physical location where computer hardware has yet to be installed. Sometimes this piece of real estate is owned by a group of enterprises that share the responsibility and cost for ownership until a member of the group needs to use the site. Then, as with an insurance policy, the needy organization can use the site according to documented agreements of usage.

**contact list:** A list of team members and key players designated to handle a crisis. This list should include home phone numbers, pager numbers, cellphone numbers, alternate residences, and (for the most critical personnel) alternate numbers for a relative who will always know where to find the critical person, and so on.


This list of home phone numbers and addresses is confidential information and must be kept locked away when not in use — and properly guarded even when in use. (If you give out the president's private numbers, nobody can save you.)

**crisis:** Any global, regional, or local event or business interruption — whether natural or human-caused — that subjects your business to these risks:

- Escalating in intensity
- Having an adverse impact on shareholder value or the organization's financial position
- Causing harm to people or damage to property or the environment
- Falling under close media or government scrutiny
- Interfering with normal operations and wasting significant amounts of management time and/or financial resources
- Adversely affecting employee morale
- Jeopardizing the organization's reputation, products, or officers, thereby threatening a negative impact on its future

**crisis management:** Intervention — including coordination by individuals or teams — before, during, and after an event to resolve the crisis, minimize loss, and otherwise protect the organization.

**crisis-management center:** A specific room or facility staffed by personnel charged with commanding, controlling, and coordinating the use of resources and personnel in response to a crisis. This is also referred to as an emergency operations center.

**crisis-management planning:** A properly funded, organized, ongoing process supported by senior management, set up to ensure the performance of three key tasks: identify and analyze the adverse impact of crisis events, maintain viable recovery strategies, and provide overall coordination of the organization's timely and effective response to a crisis.

**crisis-management team:** A group directed by senior management (or its representatives) to lead the response to an incident or crisis event. The team includes personnel from such corporate functions as human resources, information technology, facilities, security, legal, communications and media relations, manufacturing, warehousing, and other business-critical support functions.

**critical function:** Business activity or process that cannot be interrupted or unavailable for several business days without having a significant negative impact on the organization.

**critical records:** Records or documents that would, if damaged, destroyed, or lost, cause considerable inconvenience to the organization and/or would require replacement or recreation at considerable expense.

**damage assessment:** The process used to appraise or determine the damage resulting from a natural or human-caused disaster or emergency — including the number of injuries and human loss, damage to public and private property, and the status of key facilities and services.

**declaration:** The moment an enterprise officially states that it's having a situation that qualifies as a "disaster incident." This critical point in time starts the clock for implementing

procedures such as locking down the building and activating call lists, crisis-management teams, and emergency resource centers.

**disaster:** An unanticipated incident or event, usually large-scale (such as natural catastrophes, technological accidents, war, or other attacks) that causes widespread destruction, loss, or distress to an organization and may result in significant property damage, multiple injuries, or deaths.

**disaster recovery:** Immediate intervention taken by an organization to minimize losses brought on by a disaster and to begin the process of recovery. This process includes activities and programs designed to restore critical business functions and return the organization to an acceptable, workable condition.

**emergency:** A disruptive, unforeseen incident or event that demands immediate action and intervention to minimize potential losses to people, property, or profitability.

**evacuation:** An organized, phased, and supervised dispersal of people from dangerous or potentially dangerous areas to safer areas.

**evaluation and maintenance:** Process of reviewing a business continuity plan in accordance with a predetermined schedule, modifying the plan in light of such factors as new legal or regulatory requirements, changes to external environments, technological changes, test/exercise results, personnel changes, and so on.

**exercise:** An activity performed for the purpose of training and conditioning team members and other personnel to respond appropriately — with maximum performance — to a crisis.

**hotsite:** A predetermined location where computer hardware is ready and waiting to be used in the event that normal facilities are unavailable. Sometimes this is a shared resource; sometimes it's wholly owned and just waiting to be fired up.

**maintenance:** Here we're talking plans rather than equipment per se. See *evaluation and maintenance*.

**mitigation strategies:** Plans to implement the measures that lessen or eliminate the occurrence or impact of a crisis.

**mutual aid agreement:** A prearranged agreement developed between two or more entities to render assistance to the parties of the agreement. Mutual aid agreements must be obtained in writing, and you know why: When the storm hits, a handshake just won't do.

**prevention:** Plans and processes that allow an organization to avoid, preclude, or limit the impact of a crisis. The tasks included in prevention should include compliance with corporate policy, development of mitigation strategies, and the implementation of behavior and programs to support the avoidance, deterrence, and detection of crises.

**readiness:** The first step in a business continuity plan, in which the enterprise assigns accountability for the plan, conducts a risk assessment and a business impact analysis (and agrees on strategies to meet the identified needs), and forms crisis-management teams (and other appropriate response teams).

**recovery/resumption:** Plans and processes to bring an organization out of a crisis that resulted in an interruption. Recovery/resumption steps should include assessing the damage and impact, prioritizing the critical processes to be resumed, and either returning to normal operations or reconstituting operations so the business can run under a new condition.

**Recovery Point Objective (RPO)**: How current your data must be to ensure effective recovery (that is, up to the point of failure or up to the last full backup). This will determine your backup strategy.

**Recovery Time Objective (RTO)**: How quickly your company must regain its normal standard of operation to continue business. Can it get there in 6 hours, 12 hours, 24 hours? Or are we talking days or weeks here? Plan accordingly.

**response:** Executing the plan and activating the resources identified to perform those duties and services that preserve and protect life and property, as well as providing services to the surviving population. Response steps should include the recognition of a potential crisis as it develops, notification, and situation assessment — as well as crisis declaration at the appropriate time, followed by the execution of the plan and the appropriate management of communications and resources.

**risk assessment:** Process of identifying internal and external threats and vulnerabilities (and determining how likely those are to cause a disruptive event), defining the critical functions necessary to continue the organization's operations, defining the controls that must be in place to reduce exposure, and evaluating the cost of implementing such controls.

**shelter-in-place:** The process of securing and protecting people and assets in the general area in which a crisis occurs and/or wherever they are at the time of the incident.

**simulation exercise:** A test in which participants perform some or all of the actions they would take if the disaster plan were activated. Simulation exercises take place under conditions that approximate real-world conditions as closely as practicable.

**tabletop exercise:** A test method that presents a limited simulation of a crisis scenario in a narrative format. Participants review and discuss — but don't actually perform — the tasks dictated by the policy, methods, procedures, coordination, and resource assignments of plan activation.

**Terribleness Factor:** Essentially a gut reaction that flaws the thinking process. It can set in just when what you really need is a clear thought process that understands the orders of magnitude of the problem — and what resources can realistically provide meaningful relief. It's an obstacle to effective action against whatever is so terrible.

**testing:** Activities done to evaluate how well a plan meets its specified objectives or fulfills the criteria that measure its effectiveness. This process involves exercises designed to keep teams and employees effective in their duties — and to reveal any weakness in the business continuity plan.

**training:** An educational process designed to make teams and employees qualified (and proficient) in the roles and responsibilities of implementing a business continuity plan.

**vital records:** Records or documents (especially legal, regulatory, or operational) that would, if irretrievably damaged, destroyed, or lost, materially impair the organization's ability to continue business operations.

# Acronyms

Here's the alphabet soup of business continuity. Please note that some acronyms have more than one specific meaning.

**BCDR:** Business Continuity and Disaster Recovery

**BCP:** Business Continuity Plan

**BIA:** Business Impact Analysis

**BRP:** Business Recovery Plan

**DRP:** Disaster Recovery Plan

**EMT:** Emergency-Management Team; also Emergency Medical Technician

**ER:** Emergency Response

**ERM:** Emergency Resource Management; also Enterprise Risk Management

**ERP:** Enterprise Resource Planning; also Emergency Response Plans

**ERT:** Emergency Response Team; also Executive Response Team

**FUD:** Fear, Uncertainty, and Doubt

**ICS:** Incident Command Structure

**IT:** Information Technology

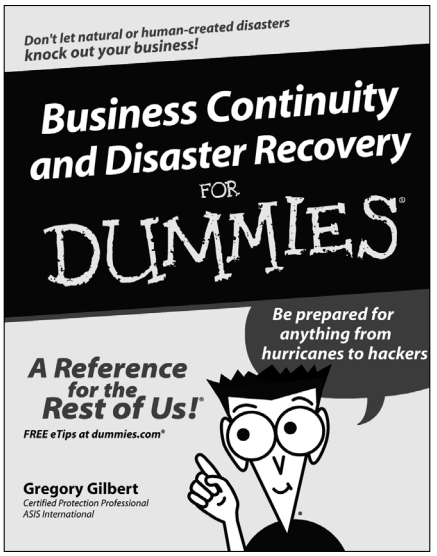
**LOB:** Line of Business

**RPO:** Recovery Point Objective

**RTO:** Recovery Time Objective

**UPS:** Uninterruptible Power System; also Uninterruptible Power Source

# Plan Ahead to Keep Your Business in Business!




0-470-03973-6 384 pgs $29.99 US

Discover how to:

- Set up procedures to prepare for anything
- Use best practices for real-world needs
- Deal with succession planning and personnel replacement

*Available July 2006 at your favorite bookseller.*

WILEY
Now you know.