

# **THE DISASTER RECOVERY HANDBOOK - A STEP-BY-STEP PLAN TO ENSURE BUSINESS CONTINUITY AND PROTECT VITAL OPERATIONS, FACILITIES, AND ASSETS**

## **Contents**

**Foreword xi**

**Introduction xiii**

### **PART 1 THE PLAN**

This section shows you how to get started with the nuts and bolts of developing your disaster recovery plan.

#### **CHAPTER 1 Getting Started: Overview of the Project**

Some companies live and breathe proper project planning and the methodical construction of business processes. A team made up of the right people using proper Project Management processes will help ensure the success of your disaster recovery project.

#### **CHAPTER 2 Risk Assessment: Understanding What Can Go Wrong**

A risk assessment is the key to your disaster plan. It identifies what risks you need to address. It breaks your risks into five layers ranging from natural disasters down to a crisis at your desk.

#### **CHAPTER 3 Build an Interim Plan: Don't Just Sit There, Do Something**

Some projects are like a bad lunch they never seem to go away. What can I do until the plan is completed? This chapter identifies actions that you can do today to assemble a useful interim plan to provide some initial protection. Everything you do here is needed in the final document. If you read no other chapter, at least read this one.

#### **CHAPTER 4 Emergency Operations Center: Take Control of the Situation**

In the event of a disaster, there must be a single place where people can call to report problems and find out what is going on. We will describe the sort of things required in an emergency operations center (sometimes called a "war room"), and how it might run.

#### **CHAPTER 5 Writing the Plan: Getting It Down On Paper**

Here is where we lay a bit more groundwork for the plan. We establish a standard format for the documents and explain what needs to be included-and excluded from a plan.

#### **CHAPTER 6 Testing: Making Sure It Works**

A plan is a wonderful thing but until it is tested and debugged, it should not be relied upon. Testing can be formally done or can be incorporated with other maintenance activities. In either case, the results of using a plan should be recorded. Testing a plan is an excellent way to familiarize your team with your plan and to gain their ideas on improving it.

### **PART 2 THE ASSETS**

This section discusses the various assets most firms have to protect and tells you what you need to know to make sure they're covered in your disaster recovery plan.

#### **CHAPTER 7 Electrical Service: Keeping the Juice Flowing**

It is hard to imagine work without electricity. We use it constantly at home (if for nothing else but to keep the clocks on time). We use it all day at work. We have all also experienced the effects of a power outage. What should our workers be doing if the lights go out?

#### **CHAPTER 8 Telecommunications: Your Connection to the World**

Few companies can quickly walk or drive to their customers' or suppliers' sites. Telecommunications makes co-ordination between companies quick and easy. It provides a medium for fax messages and also provides the data communications lines. How long can your company run without it?

**BUY ONLINE FROM: <http://www.itgovernance.co.uk/products/654>**

## **CHAPTER 9 Vital Records Recovery: Covering Your Assets**

There are many documents essential to your company's operations, such as invoices, checks, software licenses, receipts, and on and on. Some of these documents you must safeguard to meet legal and regulatory requirements. What if, what if, what if . . .

## **CHAPTER 10 Data: Your Most Unique Asset**

Data is one asset that cannot be easily replaced. No one else has the same data you do. What are the unique issues encountered when planning for data processing recovery?

## **CHAPTER 11 Networks: The Ties That Bind**

Years ago, we used over night batch programs to generate mounds of paper. Today we view our data in real time. We check inventory levels, the status of customer orders and many things we take for granted. This is all made possible by a very complex system called a data network. Lose this and it's back to piles of last night's reports for answers!

## **CHAPTER 12 End User PCs: The Weakest Link**

The personal in personal computers means that many people can develop tools to make their job easier. Along with these tools is data. Lots of company data. If it is useful, then it needs to be backed up. PCs are also a source of virus attacks on your company.

## **CHAPTER 13 Customers: Other People to Worry About**

Customers have their own problems. In a time of lean inventories, they cannot tolerate a very long delay in getting their materials or their own efforts will enter a crisis. So if they hear that you have had a disaster, might they shift their orders to someone else? This is even more of a problem if the fire was in your offices and you have a warehouse full of good that need to be sold.

## **CHAPTER 14 Suppliers: Collateral Damage**

Suppliers extend credit to you in the form of the goods. Their terms may be 30, 45, or 60 days. If they hear of a disaster, they may fear that your company will become insolvent and cease all shipments to you. They need to know the facts. You need to tell all of them.

## **PART 3 PREVENTING DISASTER**

This section discusses threats to your organization and how to include mitigation plans in your disaster recovery plan.

## **CHAPTER 15 Fire: Burning Down the House**

A thorough understanding of fire safety systems can help you to evaluate your company's existing safeguards to ensure they are current, adequate and focused on employee safety.

## **CHAPTER 16 Human Resources: Your Most Valuable Asset**

Your Human Resources department has an important role to play in Business Continuity Planning. Major business emergencies are very stressful events. From a business perspective, stress reduces the productivity of the workforce. The Human Resources department ensures that the "people side" of an emergency is addressed for the best long term benefit of the company.

## **CHAPTER 17 Backups: The Key to a Speedy Recovery**

Making backup, or safety, copies of your vital computer files is a common business practice. They are made to speed the recovery of a failed or damaged computer system. Are you sure that they will work when you need them?

## **CHAPTER 18 Virus Containment: High Tech Pest Control**

Unfortunately, new computer viruses regularly make the rounds of our far-flung data networks. This plan lists steps for implements a virus containment and remediation plan.

## **CHAPTER 19 Health and Safety: Keeping Everyone Healthy**

This should already be in place at your facility. Get a copy from your building security folks. Check it against the list we have here to see if all of the bases are covered. The safety of your workers is your number one concern.

**BUY ONLINE FROM:** <http://www.itgovernance.co.uk/products/654>

## **CHAPTER 20 Terrorism: The Wrath of Man**

While not a new phenomenon, terrorism is making the headlines. Even if your organization is not a target, you can still be shut down even if you're an innocent bystander.

**Appendix**

**Index**