IT Disaster Recovery Planning
FOR
DUMMIES®

by Peter Gregory, CISA, CISSP

Foreword by Philip Jan Rothstein, FBCI

Wiley Publishing, Inc.

IT Disaster Recovery Planning

FOR

DUMMIES®

IT Disaster Recovery Planning
FOR
DUMMIES®

by Peter Gregory, CISA, CISSP

Foreword by Philip Jan Rothstein, FBCI

Wiley Publishing, Inc.

IT Disaster Recovery Planning For Dummies®
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

Library of Congress Control Number: 2006923952

ISBN: 978-0-470-03973-1

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

About the Author

Peter H. Gregory, CISA, CISSP, is the author of fifteen books on security and technology, including *Solaris Security* (Prentice Hall), *Computer Viruses For Dummies* (Wiley), *Blocking Spam and Spyware For Dummies* (Wiley), and *Securing the Vista Environment* (O'Reilly).

Peter is a security strategist at a publicly-traded financial management software company located in Redmond, Washington. Prior to taking this position, he held tactical and strategic security positions in large wireless telecommunications organizations. He has also held development and operations positions in casino management systems, banking, government, non-profit organizations, and academia since the late 1970s.

He's on the board of advisors for the NSA-certified Certificate program in Information Assurance & Cybersecurity at the University of Washington, and he's a member of the board of directors of the Evergreen State Chapter of InfraGard.

You can find Peter's Web site and blog at `www.isecbooks.com`, and you can reach him at `petergregory@yahoo.com`.

Dedication

This book is dedicated to Rebekah Gregory, Iris Finsilver, Jacqueline McMahon, and Lisa Galoia, my personal disaster recovery team, and also to professionals everywhere who are trying to do the right thing to protect their organizations' assets.

Author's Acknowledgments

I would like to thank Greg Croy, Executive Editor at Wiley, for his leadership, perseverance, and patience throughout this project. Thank you to Christopher Morris, Senior Project Editor at Wiley, for your help. Also, thanks to Philip Rothstein for technical review and expert guidance — and for writing the Forward to this book at the last minute. And thank you, Laura Miller, for your thoughtful and effective copy editing.

And finally, heartfelt thanks go to Liz Suto, wherever you are, for getting me into this business over twelve years ago when you asked me to do a tech review on your book, *Informix Online Performance Tuning* (Prentice Hall).

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

Sr. Project Editor: Christopher Morris

Acquisitions Editor: Gregory Croy

Copy Editor: Laura Miller

Technical Editor: Philip Jan Rothstein

Editorial Manager: Kevin Kirschner

Media Development and Quality Assurance: Angela Denny, Kate Jenkins, Steven Kudirka, Kit Malone

Media Development Coordinator: Jenny Swisher

Media Project Supervisor: Laura Moss-Hollister

Editorial Assistant: Amanda Foxworth

Sr. Editorial Assistant: Cherie Case

Cartoons: Rich Tennant (www.the5thwave.com)

Composition Services

Project Coordinator: Patrick Redmond

Layout and Graphics: Stacie Brooks, Jonelle Burns, Reuben W. Davis, Melissa K. Jester, Stephanie D. Jumper, Alissa Walker, Christine Williams

Proofreader: Linda Morris

Indexer: Rebecca Salerno

Anniversary Logo Design: Richard Pacifico

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

Contents at a Glance

Table of Contents

Foreword

In the late 1960s, I was first exposed to what would later become known as disaster recovery. I was responsible for the systems software environment for a major university computer center at the time. It was at the height of the Vietnam War protests, and one of those protests spilled over to the building housing the computer room. A number of the protesters were running through the building and randomly damaging whatever was in their path. When they got to the computer room, they found a locked, heavy steel door and moved on.

It suddenly dawned on me that we had no clue — let alone plan — to deal with damage or destruction, should the protesters have gained entry to the computer room. As I thought about it and discussed this with others on the computer operations team, I realized there were many other threats and vulnerabilities that had never been discussed, let alone addressed.

Fast forward forty years. The single-mainframe data center has given way to clusters of dozens, if not hundreds, of servers and decentralized data centers; networking is often more critical than processors; dozens of computer room operators have been replaced by lights-out data centers; a week-long recovery from a data center disruption is now more likely to be an almost instantaneous failover to a backup; and disaster recovery has become a fact of life.

The bad news is that too many data center managers still have not been able to effectively address disaster recovery, whether because of lack of management commitment or lack of knowledge or lack of resources. By effectively, I mean

- A comprehensive disaster recovery plan, based on objective assessment of threats, vulnerabilities and exposure to loss
- Integration with comprehensive enterprise business continuity programs so that IT disaster recovery is consistent with overall business needs and priorities
- A meaningful exercise program, combined with training and plan maintenance, to ensure that the plan is current, realistic, and likely to work when called upon

The good news is that with Peter Gregory's new book, even a team without prior experience in disaster recovery planning can address these issues — " . . . those frustrated and hard-working souls who know they're not dumb, but find that the technical complexities of computers and the myriad of personal and business issues — and all the accompanying horror stories — make them feel helpless," as www.dummies.com points out.

Disaster recovery is not simply about Katrinas nor earthquakes nor 9/11 catastrophes. Sometimes, the focus on these monumental events could intimidate even the most committed IT manager from tackling disaster recovery planning. Disaster recovery is really about the ability to maintain business as usual — or as close to "as usual" as is feasible and justifiable — whatever gets thrown at IT. Peter's book helps to establish this perspective and provides a non-nonsense yet manageable foundation. I actually found, despite my long involvement with business continuity and disaster recovery, that he has identified many issues, techniques, and tips which I found quite useful.

While I confess I enjoyed *Italian Wines For Dummies* more, Peter Gregory's new book succeeds in taking the intimidation factor out of IT disaster recovery and offers a common-sense, practical, yet comprehensive process for analyzing, developing, implementing, exercising, and maintaining a successful IT disaster recovery program — even if he has, regrettably, failed miserably to enlighten me about Super-Tuscan wines.

Philip Jan Rothstein, FBCI, is President of Rothstein Associates Inc. (`www.rothstein.com`*, Brookfield, Connecticut USA), a management consultancy focused on business continuity and disaster recovery since 1984. He has edited or written close to 100 books and more than 200 articles, and is publisher of* The Rothstein Catalog on Disaster Recovery.

Introduction

Disasters of many kinds strike organizations around the world on an almost daily basis. But most of these disasters never make the news headlines because they occur at the local level. You probably hear about disastrous events that occur in or near your community — fires, floods, landslides, civil unrest, and so on — that affect local businesses, sometimes in devastating ways. Larger disasters affect wide areas and result in widespread damage, evacuations, and loss of life, and can make you feel numb at times because of the sheer scale of their effects.

This book is about the survival of business IT systems in the face of these disasters through preparation and response. You're largely powerless to stop the disasters themselves, and even if you can get out of their way, you can rarely escape their effects altogether. Disasters, by their very nature, disrupt *everything* within their reach.

Your organization can plan for these disasters and take steps to assure your critical IT systems survive. This book shows you how to prepare.

About This Book

IT Disaster Recovery Planning For Dummies contains a common and time-proven methodology that can help you prepare your organization for disaster.

My goals are simple — to help you plan for and prepare your systems, processes, and people for an organized response to a disaster when it strikes. You can make your systems more resilient, meaning you'll need less effort to recover them after a disaster. By using this book as a guide, you can journey through the steps of a disaster recovery (DR) project, as thousands of organizations have done before you.

This book progresses in roughly the same sequence that you must follow if your organization hasn't developed a disaster recovery plan before or if you're about to do a major refresh of outdated or inadequate plans.

How This Book Is Organized

This book is organized into four parts that you can use to quickly find the information you need.

Part I: Getting Started with Disaster Recovery

In Part I, I describe the nature of disasters and their effects on businesses. In Chapter 1, I take you on an end-to-end tour of the entire disaster recovery planning process.

I start Chapter 2 with a discussion of the various ways that a disaster can affect an organization and the role of prevention. I also include how to begin planning your disaster recovery project and emergency operations planning. Then, I show how you can quickly develop an interim disaster recovery plan that can provide some basic protection from a disaster if one occurs before you finish your full disaster recovery plan.

In Chapter 3, I take you on a deep dive into the vital first phase of a DR project — creating the Business Impact Analysis, during which you discover which business processes require the most effort in terms of prevention and the development of recovery procedures.

Part II: Building Technology Recovery Plans

Part II contains the core components of the disaster recovery plan. Chapter 4 describes how you determine which systems and underlying infrastructure support critical business processes that you identify in the Business Impact Analysis. Chapter 5 through Chapter 8 go through the work of preventing disaster and recovering from disaster in distinct groups — end users, facilities, systems and networks, and data. Chapter 9 discusses details about the actual disaster recovery plan documents — what those documents should contain and how to manage their development.

Part III: Managing Recovery Plans

Part III focuses on what happens after you write your disaster recovery plans. Chapter 10 discusses DR plan testing and the five types of tests organizations often perform. Chapter 11 describes what activities you need to do to ensure

that your DR plans stay current. Disaster prevention is the topic of Chapter 12. If you can prevent disasters, your organization is better off. Chapter 13 discusses many disaster scenarios and what each one brings to a disaster recovery plan.

Part IV: The Part of Tens

The much loved and revered Part of Tens contains four chapters that are more than mere lists. These chapters contain references to external sources of information, more reasons to develop business recovery plans, and the benefits your organization can gain from having a well-developed recovery plan.

What This Book Is — and What It Isn't

Every business needs to complete disaster recovery (DR) planning and business continuity (BC) planning.

The terms *DR planning* and *BC planning* are often confused with each other, and many people use them interchangeably. And ultimately, they're complementary activities that you have to do before a disaster occurs (in terms of planning), and during and after a disaster (in terms of response and business resumption).

IT Disaster Recovery Planning For Dummies focuses on DR planning as it relates to IT systems and IT users. In this book, I discuss the necessary steps to develop response, assessment, and recovery plans to get IT systems and IT users back online after a disaster.

This book doesn't cover business continuity planning, which focuses on generic business process resumption, as well as continuity and communications with customers and shareholders.

Assumptions about Disasters

When you think about disasters, you may think about horrific natural events, rescue helicopters, hospital ships, airlifts, the International Red Cross or World Vision, looting and mayhem, large numbers of human casualties, and up-to-the-minute coverage from CNN. You may also think of wars, terrorist attacks, or nuclear power plant explosions, and the fallout (no pun intended) that ensues. Yes, these events certainly qualify as disasters, and this book discusses the preparations that businesses can and should take to survive them.

But you also have to think about the less sensational disasters that play out almost every day in businesses everywhere — not only fires, floods, strikes, explosions, and many other types of accidents, but also security incidents, vandalism, and sabotage — not to mention IT system hardware and software failures, data corruption, and errors. All of these problems can become disastrous events that can threaten a business's survival.

Icons Used in This Book

Throughout this book, you may notice little icons in the left margin that act as road signs to help you quickly pull out the information that's most important to you. Here's what they look like and what they represent.

Information tagged with a Remember icon identifies general information and core concepts that you may already know but should certainly understand and review.

Tip icons include short suggestions and tidbits of useful information.

Look for Warning icons to identify potential pitfalls, including easily confused or difficult-to-understand terms and concepts.

Technical Stuff icons highlight technical details that you can skip unless you want to bring out the tech geek in you.

Where to Go from Here

If you want to understand the big picture about disaster recovery planning, go straight to Chapter 1. If your organization has no plan of any kind, Chapter 2 can help you get something started right away that you can have in place next week. (No kidding!) If you want to dive straight into a full-blown DR project, begin at Chapter 3.

If your organization already has a disaster recovery plan, you can turn to Chapters 11, 12, and 13, in which I discuss the activities that you need to perform on an ongoing basis.

You can also just open the book to any chapter you want and dive right into the art and science of protecting the technology that supports your organization from disasters.

Write to Us!

Have a question? Comment? Complaint? Please let me know. Write to me at petergregory@yahoo.com or phg@isecbooks.com.

You can also find me online at www.isecbooks.com.

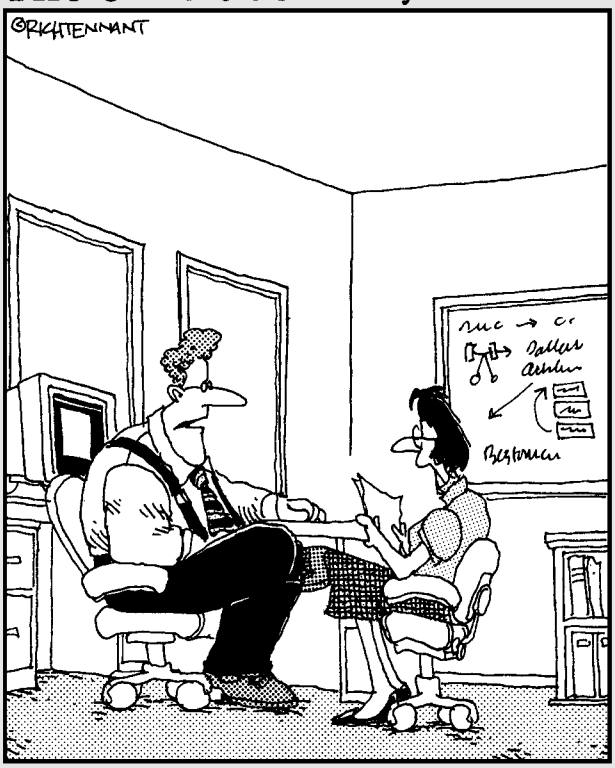
I try to answer every question personally.

For information on other *For Dummies* books, please visit www.dummies.com.

Part I

Getting Started with Disaster Recovery

The 5th Wave By Rich Tennant



"Our automated response policy to a large company-wide data crash is to notify management, back up existing data and sell 90% of my shares in the company."

In this part . . .

This part introduces the technical side of disaster recovery (DR) planning. Chapter 1 provides an overview of the entire DR process.

Chapter 2 is for organizations that have no disaster recovery plan at all. It shows you how you can make a quick start with an interim plan that provides some protection against disaster while you develop a more formal plan.

Chapter 3 covers the Business Impact Analysis (BIA) — the vital first part of the formal, long-term development of a disaster recovery plan. You use the BIA to identify the most critical business processes — those that need disaster recovery plans the most!