

***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](http://www.wiley.com)

Copyright © 2008 by Wiley Publishing, Inc., Indianapolis, Indiana

Published by Wiley Publishing, Inc., Indianapolis, Indiana

Published simultaneously in Canada

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600. Requests to the Publisher for permission should be addressed to the Legal Department, Wiley Publishing, Inc., 10475 Crosspoint Blvd., Indianapolis, IN 46256, (317) 572-3447, fax (317) 572-4355, or online at <http://www.wiley.com/go/permissions>.

**Trademarks:** Wiley, the Wiley Publishing logo, For Dummies, the Dummies Man logo, A Reference for the Rest of Us!, The Dummies Way, Dummies Daily, The Fun and Easy Way, Dummies.com, and related trade dress are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates in the United States and other countries, and may not be used without written permission. All other trademarks are the property of their respective owners. Wiley Publishing, Inc., is not associated with any product or vendor mentioned in this book.

**LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.**

For general information on our other products and services, please contact our Customer Care Department within the U.S. at 800-762-2974, outside the U.S. at 317-572-3993, or fax 317-572-4002.

For technical support, please visit [www.wiley.com/techsupport](http://www.wiley.com/techsupport).

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

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](http://www.isecbooks.com), and you can reach him at [petergregory@yahoo.com](mailto: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](http://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](http://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

---

<b><i>Foreword</i></b> .....	<b><i>xix</i></b>
<b><i>Introduction</i></b> .....	<b><i>1</i></b>
<b><i>Part I: Getting Started with Disaster Recovery</i></b> .....	<b><i>7</i></b>
Chapter 1: Understanding Disaster Recovery .....	9
Chapter 2: Bootstrapping the DR Plan Effort .....	29
Chapter 3: Developing and Using a Business Impact Analysis .....	51
<b><i>Part II: Building Technology Recovery Plans</i></b> .....	<b><i>75</i></b>
Chapter 4: Mapping Business Functions to Infrastructure .....	77
Chapter 5: Planning User Recovery .....	97
Chapter 6: Planning Facilities Protection and Recovery .....	129
Chapter 7: Planning System and Network Recovery .....	153
Chapter 8: Planning Data Recovery .....	173
Chapter 9: Writing the Disaster Recovery Plan .....	197
<b><i>Part III: Managing Recovery Plans</i></b> .....	<b><i>215</i></b>
Chapter 10: Testing the Recovery Plan .....	217
Chapter 11: Keeping DR Plans and Staff Current .....	241
Chapter 12: Understanding the Role of Prevention .....	263
Chapter 13: Planning for Various Disaster Scenarios .....	285
<b><i>Part IV: The Part of Tens</i></b> .....	<b><i>305</i></b>
Chapter 14: Ten Disaster Recovery Planning Tools .....	307
Chapter 15: Eleven Disaster Recovery Planning Web Sites .....	315
Chapter 16: Ten Essentials for Disaster Planning Success .....	323
Chapter 17: Ten Benefits of DR Planning .....	331
<b><i>Index</i></b> .....	<b><i>339</i></b>



# Table of Contents



<b><i>Foreword</i></b> .....	<b><i>xix</i></b>
<b><i>Introduction</i></b> .....	<b>1</b>
About This Book.....	1
How This Book Is Organized.....	2
Part I: Getting Started with Disaster Recovery.....	2
Part II: Building Technology Recovery Plans.....	2
Part III: Managing Recovery Plans.....	2
Part IV: The Part of Tens.....	3
What This Book Is — and What It Isn't.....	3
Assumptions about Disasters.....	3
Icons Used in This Book.....	4
Where to Go from Here.....	4
Write to Us!.....	5
<b><i>Part I: Getting Started with Disaster Recovery</i></b> .....	<b>7</b>
<b>Chapter 1: Understanding Disaster Recovery</b> .....	<b>9</b>
Disaster Recovery Needs and Benefits .....	9
The effects of disasters.....	10
Minor disasters occur more frequently.....	11
Recovery isn't accidental .....	12
Recovery required by regulation .....	12
The benefits of disaster recovery planning .....	13
Beginning a Disaster Recovery Plan .....	13
Starting with an interim plan .....	14
Beginning the full DR project .....	15
Managing the DR Project.....	18
Conducting a Business Impact Analysis.....	18
Developing recovery procedures .....	22
Understanding the Entire DR Lifecycle .....	25
Changes should include DR reviews.....	26
Periodic review and testing.....	26
Training response teams .....	26

<b>Chapter 2: Bootstrapping the DR Plan Effort . . . . .</b>	<b>29</b>
Starting at Square One.....	30
How disaster may affect your organization .....	30
Understanding the role of prevention .....	31
Understanding the role of planning .....	31
Resources to Begin Planning .....	32
Emergency Operations Planning.....	33
Preparing an Interim DR Plan .....	34
Staffing your interim DR plan team.....	35
Looking at an interim DR plan overview .....	35
Building the Interim Plan .....	36
Step 1 — Build the Emergency Response Team.....	37
Step 2 — Define the procedure for declaring a disaster .....	37
Step 3 — Invoke the interim DR plan.....	39
Step 4 — Maintain communications during a disaster.....	39
Step 5 — Identify basic recovery plans .....	41
Step 6 — Develop processing alternatives.....	42
Step 7 — Enact preventive measures .....	44
Step 8 — Document the interim DR plan.....	46
Step 9 — Train ERT members .....	48
Testing Interim DR Plans .....	48
<b>Chapter 3: Developing and Using a Business Impact Analysis . . . .</b>	<b>51</b>
Understanding the Purpose of a BIA .....	52
Scoping the Effort.....	53
Conducting a BIA: Taking a Common Approach .....	54
Gathering information through interviews .....	55
Using consistent forms and worksheets .....	56
Capturing Data for the BIA.....	58
Business processes .....	59
Information systems .....	60
Assets.....	61
Personnel.....	62
Suppliers.....	62
Statements of impact .....	62
Criticality assessment.....	63
Maximum Tolerable Downtime.....	64
Recovery Time Objective.....	64
Recovery Point Objective.....	65
Introducing Threat Modeling and Risk Analysis .....	66
Disaster scenarios .....	67
Identifying potential disasters in your region .....	68
Performing Threat Modeling and Risk Analysis.....	68
Identifying Critical Components .....	69
Processes and systems.....	70
Suppliers.....	71
Personnel.....	71

Determining the Maximum Tolerable Downtime .....72  
 Calculating the Recovery Time Objective.....72  
 Calculating the Recovery Point Objective .....73

***Part II: Building Technology Recovery Plans .....75***

**Chapter 4: Mapping Business Functions to Infrastructure . . . . .77**

Finding and Using Inventories .....78  
 Using High-Level Architectures .....80  
     Data flow and data storage diagrams .....80  
     Infrastructure diagrams and schematics .....84  
 Identifying Dependencies.....90  
     Inter-system dependencies .....91  
     External dependencies .....95

**Chapter 5: Planning User Recovery . . . . .97**

Managing and Recovering End-User Computing.....98  
     Workstations as Web terminals .....99  
     Workstation access to centralized information.....102  
     Workstations as application clients .....104  
     Workstations as local computers .....108  
     Workstation operating systems .....113  
 Managing and Recovering End-User Communications .....119  
     Voice communications.....119  
     E-mail.....121  
     Fax machines .....125  
     Instant messaging.....126

**Chapter 6: Planning Facilities Protection and Recovery . . . . .129**

Protecting Processing Facilities .....129  
     Controlling physical access .....130  
     Getting charged up about electric power .....140  
     Detecting and suppressing fire .....141  
     Chemical hazards .....144  
     Keeping your cool .....145  
     Staying dry: Water/flooding detection and prevention .....145  
 Selecting Alternate Processing Sites.....146  
     Hot, cold, and warm sites.....147  
     Other business locations.....149  
     Data center in a box: Mobile sites .....150  
     Colocation facilities.....150  
     Reciprocal facilities.....151

<b>Chapter 7: Planning System and Network Recovery</b> .....	<b>153</b>
Managing and Recovering Server Computing .....	154
Determining system readiness .....	154
Server architecture and configuration .....	155
Developing the ability to build new servers .....	157
Distributed server computing considerations .....	159
Application architecture considerations .....	160
Server consolidation: The double-edged sword .....	161
Managing and Recovering Network Infrastructure.....	163
Implementing Standard Interfaces .....	166
Implementing Server Clustering.....	167
Understanding cluster modes .....	168
Geographically distributed clusters .....	169
Cluster and storage architecture.....	170
<b>Chapter 8: Planning Data Recovery</b> .....	<b>173</b>
Protecting and Recovering Application Data .....	173
Choosing How and Where to Store Data for Recovery .....	175
Protecting data through backups.....	176
Protecting data through resilient storage .....	179
Protecting data through replication and mirroring .....	180
Protecting data through electronic vaulting.....	182
Deciding where to keep your recovery data.....	182
Protecting data in transit.....	184
Protecting data while in DR mode.....	185
Protecting and Recovering Applications .....	185
Application version .....	186
Application patches and fixes .....	186
Application configuration .....	186
Application users and roles .....	187
Application interfaces.....	189
Application customizations .....	189
Applications dependencies with databases, operating systems, and more.....	190
Applications and client systems .....	191
Applications and networks .....	192
Applications and change management.....	193
Applications and configuration management.....	193
Off-Site Media and Records Storage .....	194
<b>Chapter 9: Writing the Disaster Recovery Plan</b> .....	<b>197</b>
Determining Plan Contents .....	198
Disaster declaration procedure.....	198
Emergency contact lists and trees .....	200



Emergency leadership and role selection .....	202
Damage assessment procedures .....	203
System recovery and restart procedures.....	205
Transition to normal operations .....	207
Recovery team.....	209
Structuring the Plan.....	210
Enterprise-level structure .....	210
Document-level structure.....	211
Managing Plan Development .....	212
Preserving the Plan.....	213
Taking the Next Steps .....	213

***Part III: Managing Recovery Plans .....215***

**Chapter 10: Testing the Recovery Plan ..... 217**

Testing the DR Plan.....	217
Why test a DR plan? .....	218
Developing a test strategy.....	219
Developing and following test procedures .....	220
Conducting Paper Tests .....	221
Conducting Walkthrough Tests .....	222
Walkthrough test participants .....	223
Walkthrough test procedure .....	223
Scenarios .....	224
Walkthrough results .....	225
Debriefing .....	225
Next steps.....	226
Conducting Simulation Testing .....	226
Conducting Parallel Testing.....	227
Parallel testing considerations .....	228
Next steps.....	229
Conducting Cutover Testing.....	230
Cutover test procedure .....	231
Cutover testing considerations .....	233
Planning Parallel and Cutover Tests.....	234
Clustering and replication technologies and cutover tests .....	235
Next steps.....	236
Establishing Test Frequency.....	236
Paper test frequency .....	237
Walkthrough test frequency.....	238
Parallel test frequency .....	239
Cutover test frequency .....	240

<b>Chapter 11: Keeping DR Plans and Staff Current</b> . . . . .	<b>241</b>
Understanding the Impact of Changes on DR Plans .....	241
Technology changes .....	242
Business changes .....	243
Personnel changes .....	245
Market changes .....	247
External changes .....	248
Changes — some final words.....	249
Incorporating DR into Business Lifecycle Processes .....	250
Systems and services acquisition .....	250
Systems development.....	251
Business process engineering .....	252
Establishing DR Requirements and Standards .....	253
A Multi-Tiered DR Standard Case Study .....	254
Maintaining DR Documentation .....	256
Managing DR documents.....	257
Updating DR documents.....	258
Publishing and distributing documents .....	260
Training Response Teams .....	261
Types of training.....	261
Indoctrinating new trainees .....	262
<b>Chapter 12: Understanding the Role of Prevention</b> . . . . .	<b>263</b>
Preventing Facilities-Related Disasters .....	264
Site selection .....	265
Preventing fires .....	270
HVAC failures.....	272
Power-related failures.....	272
Protection from civil unrest and war .....	273
Avoiding industrial hazards .....	274
Preventing secondary effects of facilities disasters .....	275
Preventing Technology-Related Disasters .....	275
Dealing with system failures .....	276
Minimizing hardware and software failures.....	276
Pros and cons of a monoculture.....	277
Building a resilient architecture .....	278
Preventing People-Related Disasters .....	279
Preventing Security Issues and Incidents .....	280
Prevention Begins at Home.....	283
<b>Chapter 13: Planning for Various Disaster Scenarios</b> . . . . .	<b>285</b>
Planning for Natural Disasters.....	285
Earthquakes .....	285
Wildfires.....	287
Volcanoes .....	288
Floods.....	289

Wind and ice storms .....290  
 Hurricanes .....291  
 Tornadoes.....292  
 Tsunamis .....293  
 Landslides and avalanches .....295  
 Pandemic.....297  
 Planning for Man-Made Disasters .....300  
     Utility failures.....300  
     Civil disturbances.....301  
     Terrorism and war.....302  
     Security incidents.....303

***Part IV: The Part of Tens .....305***

**Chapter 14: Ten Disaster Recovery Planning Tools .....307**

Living Disaster Recovery Planning System (LDRPS).....307  
 BIA Professional .....308  
 COBRA Risk Analysis .....308  
 BCP Generator .....309  
 DRI Professional Practices Kit .....310  
 Disaster Recovery Plan Template .....310  
 SLA Toolkit .....311  
 LBL ContingencyPro Software .....312  
 Emergency Management Guide for Business and Industry .....312  
 DRJ’s Toolbox .....313

**Chapter 15: Eleven Disaster Recovery Planning Web Sites .....315**

DRI International .....315  
 Disaster Recovery Journal .....316  
 Business Continuity Management Institute.....316  
 Disaster Recovery World .....317  
 Disaster Recovery Planning.org .....317  
 The Business Continuity Institute.....318  
 Disaster-Resource.com.....319  
 Computerworld Disaster Recovery .....319  
 CSO Business Continuity and Disaster Recovery .....320  
 Federal Emergency Management Agency (FEMA) .....320  
 Rothstein Associates Inc. ....321

**Chapter 16: Ten Essentials for Disaster Planning Success .....323**

Executive Sponsorship .....323  
 Well-Defined Scope.....324  
 Committed Resources .....325

The Right Experts .....325  
Time to Develop the Project Plan .....326  
Support from All Stakeholders .....326  
Testing, Testing, Testing.....327  
Full Lifecycle Commitment .....327  
Integration into Other Processes .....328  
Luck.....329

**Chapter 17: Ten Benefits of DR Planning .....331**

Improved Chances of Surviving “The Big One” .....331  
A Rung or Two Up the Maturity Ladder .....332  
Opportunities for Process Improvements .....332  
Opportunities for Technology Improvements.....333  
Higher Quality and Availability of Systems.....334  
Reducing Disruptive Events.....334  
Reducing Insurance Premiums.....335  
Finding Out Who Your Leaders Are .....336  
Complying with Standards and Regulations.....336  
Competitive Advantage .....338

***Index*.....339**

# Foreword

---

**I**n 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](http://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](http://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

---

**D**isasters 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](mailto:petergregory@yahoo.com) or [phg@isecbooks.com](mailto:phg@isecbooks.com).

You can also find me online at [www.isecbooks.com](http://www.isecbooks.com).

I try to answer every question personally.

For information on other *For Dummies* books, please visit [www.dummies.com](http://www.dummies.com).

# 6

## IT Disaster Recovery Planning For Dummies

---

# Part I

# Getting Started with Disaster Recovery

The 5<sup>th</sup> 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 . . .*

**T**his 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!