BUSINESS RESUMPTION PLANNING

Second Edition

Edited by LEO A. WROBEL

CRC Press
Taylor & Francis Group
AN AUERBACH BOOK

BUSINESS RESUMPTION PLANNING

Second Edition

OTHER INFORMATION SECURITY BOOKS FROM AUERBACH

802.1X Port-Based Authentication
Edwin Lyle Brown
ISBN: 1-4200-4464-8

Building an Effective Information Security Policy Architecture
Sandy Bacik
ISBN: 1-4200-5905-X

CISO Soft Skills: Securing Organizations Impaired by Employee Politics, Apathy, and Intolerant Perspectives
Michael Gentile, Ron Collette and Skye Gentile
ISBN: 1-4200-8910-2

Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience, and ROI
Debra S. Herrmann
ISBN: 0-8493-5402-1

Computer Forensics: Evidence Collection and Management
Robert C. Newman
ISBN: 0-8493-0561-6

Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, Second Edition
Albert Marcella, Jr. and Doug Menendez
ISBN: 0-8493-8328-5

Digital Privacy: Theory, Technologies, and Practices
Alessandro Acquisti, Stefanos Gritzalis, Costos Lambrinoudakis and Sabrina di Vimercati
ISBN: 1-4200-5217-9

How to Achieve 27001 Certification: An Example of Applied Compliance Management
Sigurjon Thor Arnason and Keith D. Willett
ISBN: 0-8493-3648-1

Information Assurance Architecture
Keith D. Willett
ISBN: 0-8493-8067-7

Information Security Management Handbook, Sixth Edition
Harold F. Tipton and Micki Krause
ISBN: 0-8493-7495-2

Information Security Management Handbook, Sixth Edition, Volume 2
Harold F. Tipton and Micki Krause
ISBN: 1-4200-6708-7

Information Security Management Handbook, 2008 CD-ROM Edition
Harold F. Tipton and Micki Krause
ISBN: 1-4200-6698-6

Insider Computer Fraud: An In-depth Framework for Detecting and Defending against Insider IT Attacks
Kenneth Brancik
ISBN 1-4200-4659-4

Mechanics of User Identification and Authentication: Fundamentals of Identity Management
Dobromir Todorov
ISBN: 1-4200-5219-5

Official (ISC)2 Guide to the SSCP CBK
Diana-Lynn Contesti, Douglas Andre, Eric Waxvik, Paul A. Henry and Bonnie A. Goins
ISBN: 0-8493-2774-1

Oracle Identity Management: Governance, Risk, and Compliance Architecture, Third Edition
Marlin B. Pohlman
ISBN: 1-4200-7247-1

Software Deployment, Updating, and Patching
Bill Stackpole and Patrick Hanrion
ISBN: 0-8493-5800-0

Testing Code Security
Maura A. van der Linden
ISBN: 0-8493-9251-9

Wireless Crime and Forensic Investigation
Gregory Kipper
ISBN: 0-8493-3188-9

AUERBACH PUBLICATIONS

www.auerbach-publications.com
To Order Call: 1-800-272-7737 • Fax: 1-800-374-3401
E-mail: orders@crcpress.com

BUSINESS RESUMPTION PLANNING

Second Edition

Edited by LEO A. WROBEL

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business
AN AUERBACH BOOK

Auerbach Publications
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

© 2009 by Taylor & Francis Group, LLC
Auerbach is an imprint of Taylor & Francis Group, an Informa business

No claim to original U.S. Government works
Printed in the United States of America on acid-free paper
10 9 8 7 6 5 4 3 2 1

International Standard Book Number-13: 978-0-8493-1459-9 (0)

This book contains information obtained from authentic and highly regarded sources. Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors and publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.

Except as permitted under U.S. Copyright Law, no part of this book may be reprinted, reproduced, transmitted, or utilized in any form by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying, microfilming, and recording, or in any information storage or retrieval system, without written permission from the publishers.

For permission to photocopy or use material electronically from this work, please access www.copyright.com (http://www.copyright.com/) or contact the Copyright Clearance Center, Inc. (CCC), 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400. CCC is a not-for-profit organization that provides licenses and registration for a variety of users. For organizations that have been granted a photocopy license by the CCC, a separate system of payment has been arranged.

Trademark Notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

Library of Congress Cataloging-in-Publication Data

Wrobel, Leo A. (Leo Anthony)
Business resumption planning / Leo A. Wrobel. -- 2nd ed.
p. cm.
Includes bibliographical references and index.
ISBN-13: 978-0-8493-1459-9 (alk. paper)
ISBN-10: 0-8493-1459-3 (alk. paper)
1. Crisis management. 2. Business planning. 3. Data recovery (Computer science) 4. Emergency management. I. Title.

HD49.D48 2007
658.4'7--dc22 2007013876

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the Auerbach Web site at
http://www.auerbach-publications.com

Dedication

This book is dedicated to **Sharon M. Wrobel**, without whom this project would have been a largely unrealized dream. Sharon worked tirelessly in the final editing of my submissions and those of numerous other contributors. More important, Sharon actually "came of age" not only as an editor but also as an active author in her own right, having written a significant portion of this book on her own. Don't be surprised to see a disaster recovery book by her in the future.

Finally, I would especially like to thank Sharon not only for her work in this project, but for her 31 years of marriage to me, which has included 7 children and 10 grandchildren. Indeed, many dreams would have remained unfulfilled if not for her.

Leo A. Wrobel

Contents

Introduction ix
About the Editors xiii
Contributors xv

1 So, You Want to Write a Disaster Recovery Plan 1
LEO A. WROBEL

2 Understanding Business Impact Analysis 23
FRANK W. GESINSKI AND LEO A. WROBEL

3 Selling Management with a Compelling Business Impact Analysis and FMEA (Failure Mode Effects Analysis) 57
RADI SHOURBAJI

4 Leveraging Internal Resources to Complete the Plan 77
LEO A. WROBEL

5 Developing Operating and Security Standards 99
LEO A. WROBEL

6 Documenting the Plan — What to Include 133
LEO A. WROBEL

7 Writing a Telecommunications Recovery Plan 181
LEO A. WROBEL

8 Notification, Teams, Recruitment, and Testing 241
LEO A. WROBEL

Special Section — Legal Implications of Not Adequately Planning 269

9 Legal and Regulatory Requirements Regarding Disaster Recovery Planning 271
EDDIE M. POPE

10 Sarbanes–Oxley Act of 2002 337
DAVID P. MOWERY

Special Additional Section: Regulatory Issues and How They Affect Business Continuity (BC) Programs 353
TRACY COWAN
RICK HOLLER

Appendix 1: Now Pull It All Together and Write a Great Disaster Recovery Plan 359
LEO A. WROBEL

Appendix 2: Partial Glossary of Telecommunications Terms and Acronyms 441
LEO A. WROBEL

Index 487

Introduction

It's 3 A.M. on a dark, rainy night, and you get the call you have always dreaded. There has been a gas explosion at the company. The building has been reduced to ashes and flames. Your first thought is to call Bob. Bob is your resident network genius. Bob knows where all the wires go, knows who the vendors are, and has every critical phone number committed to memory. If you are going to recover from this disaster, you need Bob.

You dial the phone and Bob's wife, half-asleep, answers. You apologize, but explain that there has been a terrible explosion at the company. You explain that you need Bob to come to work now. *Just when you think things can't be any worse, Bob's wife responds with four words that prove to you that it can: "Bob* is *at work!" Now you have* another *problem to deal with! You may be frantically thinking, "But I am a network manager, not a grief counselor! How can I deal with a hysterical wife? What should I do! If* only *I had planned ahead … !"*

I have used this story many times over the years because it graphically illustrates one aspect of contingency planning—how to call-out employees—in a manner that makes the issue easy to remember. There are thousands of other issues to remember, and we hope to use the same kinds of "memory joggers" in this book to try to assure you that as many of them are remembered as possible. We do this using every trick, scheme, manipulation, and example. And, by the way, we hope to make learning this material fun. However we attempt this, we make it possible for you to recall what you read here, and become a more effective contingency planner in the process. Given the complexity of the task, you will need all the help you can get!

Addressing the many issues that confront the network recovery planner today is a mind-boggling task. Presently, organizations are almost totally dependent upon their networks for operations and cannot operate without their functionality. It involves much more than the technical stuff like LANs, WANs, MANs, FANs, CANs, and PANs (those really are technical terms of art for local, wide, metropolitan, foreign, campus, and personal area networks). Then you have the whole world

of telecommunications jargon like T1, T3, xDSL, and things like POTS (Plain Ordinary Telephone Service).

Anyway, getting back to the example above with Bob, many companies' "first alert" call-out procedures are seriously deficient. Bob may in fact have just been out tipping a few beers with friends. Then again, maybe not. The point is, grief counselors are one component of successful "first alert" procedures and need to be on your call-out lists. (You do *have* first-alert procedures and call-out lists, don't you?) If not, this book can help you get them in place—today. It will also address thousands of other "loose ends" in your contingency plan in the process.

You can't possibly know everything about contingency planning, nobody can. From a theoretical standpoint, the number of possible disasters will always equal n + 1, with n being the number of possible scenarios covered in your plan. We will show you how to respond to most of them and have a plan for almost anything that can or will happen. With the help of this book you can be secure in the knowledge that everyone that needs to be involved in a disaster will be involved. You then can concentrate on what is most likely your specific task, **restoring the technology**. Just so you don't feel left out, we offer you a plethora of information, tips, and templates on that task as well, whether it be computers, telecommunications, or infrastructure you're addressing. We also make some assumptions in this book with regard to restoring technology:

1. In all probability, nobody knows the specific technology better than you do. In fact, you are probably your organization's "Bob" or you would not even be reading this book. It takes the effort of a large, coordinated team, however, to recover from a major disaster. This book is your first step to coordinating that effort, to safeguarding your company … and your job.
2. We provide you with a detailed and comprehensive guide. No, it does not contain *everything*, probably nothing can. It is absolutely *loaded* however with real-life case studies and examples that illustrate the vulnerabilities of today's mission-critical systems. From a burst pipe in a telephone closet to a terrorist's chemical or biological strike, we explain in detail the proactive steps you should be taking now to first assess your exposure, then eliminate it. As a matter of fact, we dedicate whole chapters to "war stories" and real-life examples from people who had disasters and survived—or did not.
3. This book builds on concepts first published in 1997 in the successful first edition of *Business Resumption Planning.* This new edition, *Business Resumption Planning—Second Edition* (BRP2E), updates all the best parts from the first series, like sample recovery plans and standards documents. It is loaded with a sizeable amount of new material as well, including:
   - Updated techniques to conduct a Business Impact Analysis (BIA) to accurately measure the effect of a disaster on your organization.
   - Updated techniques for conducting a Failure Mode Effects Analysis (FMEA) that can accurately compute the probability of a disaster in all

types of automated systems. This is intended to channel your limited resources where they are needed most, and avoid wasting your time on things others may have already done.

- How to recover from ground zero. For years, companies believed they would not have to recover from a "smoldering hole in the ground." That has all changed. Oklahoma City, the World Trade Center, and Katrina have forced a rethinking of conventional wisdom. What does your plan need to "recover from rubble?" You will learn how your business can survive megadisasters in this book.
- Are your service providers prepared to recover after a disaster? A detailed checklist is included and should be an indispensable component of any telecom service Request for Proposal (RFP). This is particularly important (in the United States, anyway) as the telephone provider is rebuilding its monopoly after 20 years of competition from multiple vendors. What new vulnerabilities are being introduced, as the country will largely be a one telecom vendor show? (I can't tell you the name of the company so I'll just give you its initials: AT&T!)
- What are the legal ramifications of failing to plan? Liability issues once limited solely to the corner office could now affect you. Find out how in a captivating new chapter by Eddie M. Pope, Esq. He is a lawyer, but you are going to like him anyway (sorry, Eddie, I couldn't resist).
- How does the Sarbanes–Oxley Act of 2002 (SOX 2002)impact your planning effort? What specifically does an auditor, accountant or CPA need to know? Bolster your knowledge by reading the chapter by David P. Mowery, CPA, and be ready when those auditors come around. Dave, besides being another lifelong friend like Eddie, goes far beyond the perspectives of the average bean counter and his perspectives on SOX 2002, in particular, are an eye opener.
- We show you how to recruit the talent you need and take a "guerilla warfare" approach to finding free materials in the public domain. This perspective comes from all the authors, who besides being experts in many aspects of recovery planning, are also great scroungers. We understand many of you are working with limited personnel and financial support so we offer some tips on how to develop a plan in spite of these constraints. We hope that, in this regard, this book pays for itself many times over and helps you further your plan despite the budget pressures that affect all of us. For example, what can disaster recovery services providers like IBM and SunGard do for you? Should you hire a consultant? Can your external or internal auditor actually be an ally rather than adversary? How do you find money for your plan, and how do you get management to buy off on it?
- How long could your company survive a total cutoff of communications or computer services? We detail how to accurately compute your exposure

in the ultimate terms management understands—dollars. Be the "godfather" of disaster recovery in your organization. Make management an "offer they can't refuse" which guarantees *funding* and support for your organization's planning effort.

And FINALLY …

We are proud to provide you detailed, step-by-step plans and templates for assessing vulnerability in WANs, Open Networks, Physical Facilities, Environmentals, and a host of Enhanced Services. We show you how to develop and write Operating and Security Standards for emerging, existing, and legacy systems. And, yes, we also have some great examples in there of air-tight "first alert" procedures so if you have to call that "Bob" in your company, this process will go smoothly. We hope you find BRP-2E to be a useful and indispensable part of your recovery planning effort and invite your comments—and contributions for future editions!

About the Editors

Leo A. Wrobel has 25 years of experience with a host of firms engaged in banking, brokerage, heavy manufacturing, telecommunications services, and government. A noted author and technical futurist, Leo is responsible for many technological firsts, including the first microwave "bypass" shot in Dallas (1985). He was the first person in Dallas to run T1 telephone traffic over a cable television system in an agreement he pioneered in 1985. Leo also served ten years as an elected mayor and city councilman of a Dallas suburb (but says he is "better now").

A sought-after speaker, Leo has lectured throughout the United States and overseas in Israel, South America, and other locations, as well as appearing on several television news programs, including KLRU's *Austin at Issue.* A knowledgeable and effective communicator, he has combined his political and technical savvy in repeated engagements in order to get things done, even at the highest policy levels.

Leo served as president and CEO of Dallas-based Premiere Network Services, Inc. from 1986 until 2005. Prior to this, he was director, Network Planning and Engineering, for Lomas and Nettleton and held technical positions at AT&T in its former Long Lines subsidiary. He is a Vietnam-era veteran (sergeant, United States Air Force) and holds degrees in electronic systems technology and telecommunications systems technology from Los Angeles City College as well as in business and public policy from the University of Texas at Dallas. Leo is a member of the I.E.E.E., Independent Telephone Pioneers of America, Southwestern Bell Pioneers, Association of Contingency Planners (ACP), and other noteworthy organizations.

An active author and technical futurist, he has published 11 books and more than 500 trade articles on a wide variety of technical subjects, including: *Understanding Emerging Network Services, Pricing, and Regulation* (Artech House Books), "Managing Emerging Technologies for Competitive Advantage" (*Computer Economics, 1995*), the *Definitive Guide to Business Resumption Planning* (Artech House Books), and *The MIS and LAN Managers Guide to Advanced Telecommunications* (I.E.E.E. Books). Leo welcomes questions and can be contacted at http://www.b4Ci.com or by phone at (214)CALL-LEO, (214)-225-5536.

Sharon M. (Ford) Wrobel served as corporate secretary and director of personnel for Premiere Network Services Inc. prior to joining b4Ci, Inc. in 2004. During that time, Sharon was instrumental in getting Premiere certified as the first CLEC to be certified in all 50 states, by aiding in filings and attending hearings. She also engaged in extensive research for Premiere, a function she continues with b4Ci as vice president of business development.

Sharon is a past president of the Ellis County Early Childhood PTA and the Ovilla Lions Club. She attended the University of Maryland and El Centro College in Dallas and was trained as a registered nurse before joining Leo in business in the late 1990s. Sharon has also served as a public official by accepting appointments to the local Planning and Zoning Commissions and the Historical Commission.

Contributors

T. Scott Atkinson, President
ICSI Consulting
San Antonio, Texas

Tracy Cowan
ICSI Consulting
San Antonio, Texas

Rick Holler
San Francisco, California

John Lyons
Senior Marketing Engineer
Jonestown, Texas

Frank W. Gesinski, CBCP
Independent Consultant
Tulsa, Oklahoma

David P. Mowery, Principal and CFO
Tel*LAW*Com Labs, Inc.
Ovilla, Texas

Ed M. Pope, Esq.
Austin, Texas

Radi Shourbaji, President
Network and Systems Professionals Association (NaSPA)
Milwaukee, Wisconsin

Chapter 1

So, You Want to Write a Disaster Recovery Plan ...

Leo A. Wrobel

Contents

What Is a Disaster? 2
Finding the Resources to Complete the Plan 3
How Does One Begin? 5
Summary 10
Chapter 1 Worksheets 11

Uh oh, the system is down. But which system? Maybe it's a mainframe, maybe it's an "open" system in use by a busy customer service agent. Maybe it's not the "system" at all, but the telecommunications link that connects the user to a system. In any event, the automated system that was originally designed to serve us has now become an irritant in our lives, or maybe something worse.

Welcome to the world of disaster recovery planning. If you have drawn the short straw and been tasked with producing a plan for your organization, then I am both happy and sad for you. It will be an interesting and challenging endeavor!

Today, disaster recovery plans encompass every type of automated system, including Mainframes, midrange computers "open" systems, desktop devices, and perhaps even PDAs (personal digital assistants). All of these play a role in the conduct of today's business, and all of them will have to be considered in your plan. But that's not all. Advanced telecommunications systems, including the World Wide Web, support voice and data connections to these systems and make them revenue generators by making them more available to customers. Just imagine! Mission-critical applications using the Internet — a network that nobody owns!

The auditors of years past would have a cow. Today it's all part of doing businesses. Consider just a few examples of this.

1-800-FLOWERS. This is a number for a company that obviously sells flowers. Now, forget the number. Get the picture? This company enjoys a significant competitive edge by providing patrons with a nationwide "local" telephone number that is easy to remember (especially for guys who mess up and forget their anniversary). According to folklore, this company was acquired in the 1990s when it was on the brink of bankruptcy. Today, they do better than half a billion dollars a year on guys like me. And that's the *old* news.

The Internet has opened up methods of business that were inconceivable even five years ago. I don't go to the store much anymore. I shop online or visit Ebay. So do many others. What's more, banks and financial services are getting into the action in a big way too. When was the last time you walked into a bank to conduct business, or into a broker's office to trade stock?

I could go on all afternoon covering the changes just in the years since the first edition of *Business Resumption Planning* was published. In this second edition, we catch up a lot on the technology. Anyone can attest that technology has changed dramatically in the last nine years. At the same time, we are reintroducing tried and tested disaster recovery planning fundamentals. These fundamentals have, astoundingly, changed very little, sometimes over 30 years or more. We will cover that fact in this book as well, as it will save you a lot of legwork as you write your plan.

What Is a Disaster?

Clearly, the answer to this question changes with time. Nine years ago when this book first published, Oklahoma City, Hurricane Katrina, the Tokyo Subway incident and, of course, 9/11 had not occurred. These and other events have changed and colored our definition of disasters to the point where they have perhaps permanently altered our very psychology as a nation. What has remained constant over this time is the fact that computers and communications are more of an indispensable component of our economy than ever. Whole new classes of "businesses without storefronts" have appeared. These all depend almost exclusively on one form of "value-added-sand" or another, whether these silicon chips are computer based or the telephone.

The classical scenarios of fire, flood, earthquake, tornado, sabotage, and other disasters still apply. Buildings still burn and get flooded. The impact of such disasters, however, is intensified today when they take enabling technologies with them and potentially affect millions of people.

At the 100,000-ft level we can split disasters into three categories: natural causes, human error, and intentional causes. Virtually all kinds of disasters can be grouped into one of these categories. A fourth category can also be added called

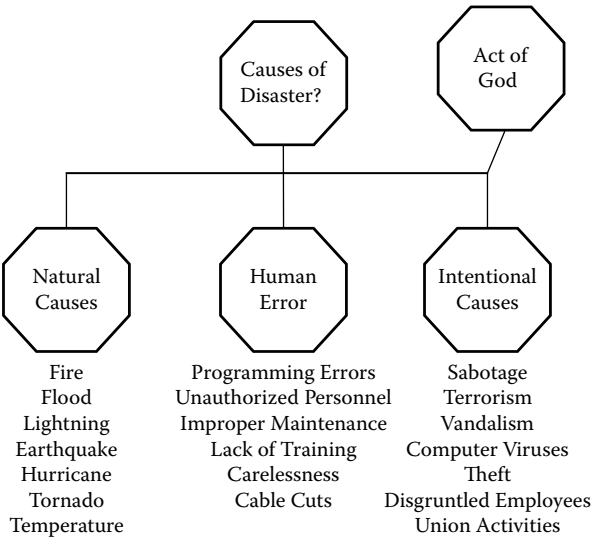


Figure 1.1 Causes of disaster.

acts of God as a catch-all for disasters that defy classification (the legal term for this is *force majeure*). With all this said, let's jump right in. (See Figure 1.1.)

Finding the Resources to Complete the Plan

Whether your responsibility is as a LAN/open systems manager, telecommunications manager, mainframe systems manager, or other Infrastructure Manager, planning for catastrophic disruptions in the systems you control should be an integral part of your job. There are portions of this task that can be shared between departments, spreading the workload over more people, the objective being to hopefully come up with a superior plan faster.

Consider the fact that the lines separating the voice communications, data communications, and local area network departments are becoming more blurred than ever. Just a few years ago, when the Internet was down you lost only data services. Today, with the advent of VoIP (Voice integrated with data over the same network) phone service, many companies now lose their voice and data services when an internal, previously all-data network is down.

Reflective of these changes, equipment component categories themselves are becoming blurred as well. (First, consider that one network resides "in house" and another very similar network that resides "out house.") Ed Pope and I predicted that this would happen when we wrote our 1993 book *Understanding Emerging Network Services, Pricing and Regulation*. We predicted that fiber optics would

make telecommunications like Doritos (eat all you want, we'll make more) and that the network would become increasingly independent of whether the services were voice, data, or something else. We predicted that it would come down to how many "gigacells" would traverse the network and how the providers would manage them. You may recall that in 1993, the only technology that would reliably manage "gigacells" was ATM (Asynchronous Transfer Mode).

As it turned out, it is gigapackets that are managed today, as IP (Internet protocol) has won over ATM in most environments. Even so, it's amazing to see the degree to which today's IP networks have become multipurpose and completely independent of whether the payload is voice, data, image, video, or something else. That fact needs to be reflected in our recovery plans today, because routers, for example, now do more than only data. Switches do more now than only voice. In some environments, physically speaking there is literally no difference between the two because Doritos are Doritos and data packets are data packets. Eat all you want, we'll make more. Our economy has had an insatiable appetite over the last few years. This brings me to another point:

As it is no longer necessary to physically segregate many types of equipment as we did in days past (voice is really data; data is really data, too — understand?), the recovery-planning task has in some ways gotten easier. Think about it.

- Traditional telecommunications switches (those that are still left after IP!) are large computers and require the same protection and operating standards as mainframes.
- Mainframes in turn don't require a lot of the excess baggage they once used to require, like chilled water, 400 Hz power, etc. They can sustain themselves just fine in a well-conditioned space, not necessarily the "environment" that they used to require.
- Many "mission-critical" frontline applications continue to migrate to the "open" server environment. Therefore, operation and security standards that used to apply only to the mainframe should now apply to the servers as well. It's not the platform that's important, it's the application the platform supports, and how long the company can survive without it.

Chances are that all three systems, telecom, open systems, and mainframes, reside today in the same equipment rooms in your organization. That means if you protect the room, you have protected all three technologies. We will discuss in detail about how you can share the duty with other departments (and the cost) in later chapters. For the remainder of this chapter, we will provide some basic information about what your planning objectives should be, what it should cost, where to get resources, and where you should start.

How Does One Begin?

I think it's safe to say that most of the people initially tasked with responsibility for a disaster recovery plan by their organizations will not really know where to start. Indeed, the responsibility to maintain the integrity of the business in the event of a natural disaster, catastrophic human error, major system failure, or even a terrorist attack can be a daunting task at first glance. When you think about it, however, as technologists we get presented with all kinds of difficult impossible deadlines and most of the time we do just fine. So what else is new?

The key to a successful project, as any good project manager will tell you, is organization. You will need to define your goals and expectations, set clear objectives, and have a measurement in place to gauge your progress. To put it another way, you need a project plan for the recovery plan.

You will undoubtedly have financial constraints and probably will not have all the people you need for the project. Been there. Done that. It is possible, however, to get a plan in place even so, and at reasonable cost, if the project manager:

1. Secures firm management commitment before beginning
2. Uses expensive resources such as outside consultants judiciously to accomplish specific and well-defined goals
3. Exploits the internal resources already available in the company
4. Has a good project plan and means to measure progress

Consider the following diagram (Figure 1.2). It illustrates a four-step process to achieve the goals set forth earlier.

I have personally seen this type of plan utilize as few as three steps, and as many as six. You know your organization best, so you decide. For the purposes of this article I have settled on four. In this case they are as follows:

- **Phase I** Business Impact Analysis (BIA) and Executive Commitment
- **Phase II** The Standards Phase
- **Phase III** Documentation of the Recovery Plan
- **Phase IV** Integration with Corporate Plan

Phase I — Business Impact Analysis and Executive Commitment

The idea in Phase I is to utilize the most expensive resources as little as possible, but to accomplish some very complicated goals. One of the first tasks includes a preliminary Business Impact Analysis (BIA). You are probably not going to be privy to a lot of the details of the core business in your organization, because chances are you work in technical services. Even if you find out about details and can describe

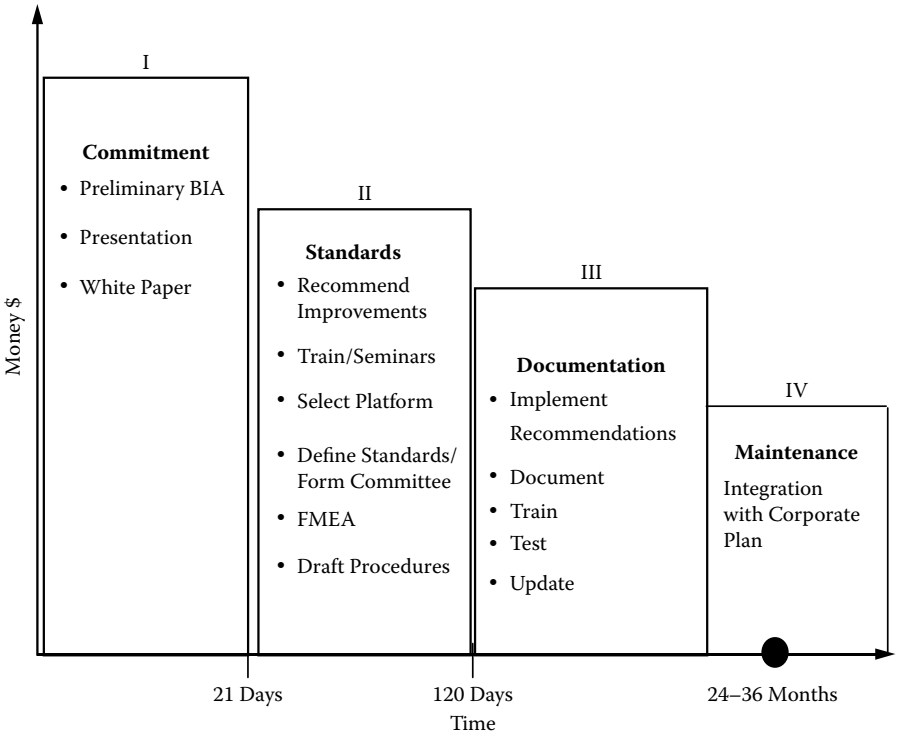


Figure 1.2 Four phases of the planning process.

to them, management may not believe you. Management will believe the right consultant, however.

Why does management believe consultants but not the company's own people? It doesn't seem fair, does it? In fact, count the number of times you have chanted ad infinitum that "this must be a priority … " only to have Ernst and Young come in and play a round of golf with your CEO. On Monday the CEO comes in with the enthusiasm of a Southern Baptist preacher proclaiming the gospel that "this must be a priority!" — the same advice, incidentally, that you have been giving for the last two years.

What does the Big 4 Consulting Company have that you don't? After all, isn't it logical that you would know more about your business than they do?

What they have that you don't have (but can acquire) is the ability to speak to management in terms they understand. That means business terms, not technical terms. The role of a good consultant is to borrow management's watch to tell them what time it is. You are the watch. The outside consultants are going to come to you for a lot of this information anyhow. Don't get me wrong, "Big 4" consultants are very good at what they do. With a little coaching, you can use that to your advantage.

Oh, and by the way, if you as the reader are a Big 4 consultant, there is something here for you too. This same advice is a great way to package your services so

that client companies can afford you. You will also delight your client because the techniques described here will not give your client a fish, they will teach your client to fish. Nothing makes for a better and more satisfying consulting engagement than the sense from your client that they have truly learned from you.

Getting back to the project manager, remember that high-end consulting resources are expensive. You will need to limit their participation to certain essential, clearly defined goals. In the meantime, learn everything you can from the consultant, first and foremost because it broadens your skill set and makes you more valuable, even on other non-disaster-recovery-related projects and, second, so that you can become the flag bearer for the disaster recovery project in Phase II — not the expensive consultant.

Let's assume this first phase is being performed by a high-level consultant, like Price Waterhouse, Ernst and Young, or one of the others. Bring your wallet. Your organization is going to pay a high rate for the consultants. But there is no reason that it cannot limit the hours somewhat and use this expensive resource judiciously. In other words, use the consultant but only for a relatively short time. During this phase, the following action items are undertaken.

The All-Important Executive Pitch

As I stated earlier, consultants carry credibility with executive management and speak a language in terms executive management understands. This means that when properly utilized, consultants can be very useful for securing financial commitment from management.

First, the consultants may conduct a preliminary business impact analysis (BIA). They may also make the executive pitch complete with some very classy audiovisual material. They may also produce an executive white paper with lots of graphs that condense 5000 words into four pages (seriously, another very useful talent that a good consultant will possess). The consultants will make the compelling point that disaster recovery is important, presenting all the reasons management needs to fund and endorse the project. All for only $500.00 an hour.

Oh, well, I was probably doing a pretty good job selling you until I got to that hourly number. So now what do you do?

I remind you again — that you are an *experienced project manager*. This will not be the first or the last time you will have to work within financial constraints. It's also not the first time you have been tasked with a complex project. The name of the game is what it has always been: resource optimization. Sure, consultants will be an expensive resource, but you will only utilize them to accomplish specific objectives in order to keep the cost down. The most important of these is to sell your boss.

Pros and Cons of Consultants

One course of action you can consider if you can't afford a high-powered consultant to pitch the top brass is to do the executive presentation yourself. There are career advantages from the visibility you will receive; after all, for many companies disaster recovery planning is a board-of-directors-level issue. If, on the other hand, this prospect intimidates you, you will probably want to get someone to champion it for you. If you end up doing it yourself, there are a few tips on how to do it presented later in this book. The important thing is not to be intimidated by this project simply because it is something you have not done before. Think of it as a new learning experience that will elevate your standing as a technologist and broaden your horizons.

Presenting the Case to Management

Ironically, you have to actually ask permission to plan. Without management buy-in and endorsement on the project (as well as funding), you are spinning your wheels. At best you can expect to be assigned the project to complete in your copious spare time, or at home in the evening on the kitchen table. If you expect to have people, money, and resources to complete a plan, there are some steps to take first. The first one is to sell your boss. The second one is permission to plan. When asking permission to plan, there are three possible answers. Which one answer do you think is given the most by management?

A. Yes
B. No
C. Let's study this some more.

Now, why do you suppose "C" is the answer most often given? Stated another way, have you had a disaster recovery project that lasted five years? This is, in part, why. Management never gets off the dime in supporting the plan and the organization "studies" it forever. This is not to hang the blame on management, however. This problem is usually because technical people are not always very adept at presenting to management in terms management understands. A consultant can help because they are adept at these presentations. This is discussed in more detail in the following chapters.

For the moment, however, as this is only an overview, let's return to our four-step process defined previously. We are now on Phase II.

Phase II is more "nuts and bolts" in orientation and, hopefully, less expensive. It centers on information gathering and standards.

Phase II — The Standards Phase

At the 100,000-ft level, activities undertaken in Phase II might include:

- Recruiting the Planning Team
- Training staff and hosting seminars
- Developing operating and security standards
- Gathering information via interviews and questionnaires
- Identification of critical databases to import into the plan
- Making long-term technology recommendations and making capital requests
- First draft of the actual plan
- Beginning to integrate the technology plan into the overall corporate plan

Recruiting Allies to Back Up the Need…Who Does Management Hold in Confidence?

1. Corporate Controller/CFO
2. General Counsel
3. Vice President Sales
4. Vice President Marketing
5. Vice President Production
6. Subsidiary/Corporate Officers
7. Vice President MIS/Technical Services

Phase III — Documenting the Recovery Plan

After completion of Phase I and Phase II (typically 90 to 120 days), you will finally begin writing the plan. This is not to say you will have no plan during the ensuing 120-day period. Indeed, many things like equipment inventories and personnel call out lists are actually compiled in Phase II. If you do things right, you should be able to compile something good enough to get the auditors off your back in 90 to 120 days. A complete plan, however, takes two years or more to finish. It is almost always under refinement and, besides, you can't trash all the equipment you have today and buy new equipment. You have to phase out what you have and replace it with equipment having fault-tolerant or disaster-resistant characteristics. That takes time, but eventually it will get done.

Phase IV — Integration with Corporate Plan

You can't expect to plan in a vacuum. Consider the elemental issue of who "owns" the building? The data center manager may think he or she owns the building. There is a guard in a blue suit with a badge, however, who sits at the front door, and this person has different ideas. You may have a landlord. You can't just plan based on your department; you must involve others. Your plan will eventually have to be integrated into the Corporate Recovery Plan. This is part of what goes on in Phase IV. This is the time you will test and verify your plan. When you refer back to the four-step diagram, do you notice how the cost decreases with each subsequent phase? This is because you are using fewer and fewer resources like outside consultants, and you are doing (and learning) more and more of the work yourself.

Summary

Wow, we make it sound so easy, don't we? Similar to any complicated project, the devil is in the details. That's why even though we have laid out a thumbnail sketch of a plan and how to implement it, the remaining several hundred pages will dive right into the details. These include not only the obvious things, like budget and technology limitations, but the less obvious ones as well, such as departmental "turf issues" and other politics.

In summary, often the most difficult part of the planning process is simply getting off square one, and starting. We hope this book helps you do that. You have handled complex projects before, so don't be afraid of this one. Disaster recovery planning is a thoughtful and methodical process. As most experienced managers have dealt first hand with projects of equal or greater complexity, most are up to the task of producing a plan. Sometimes, though, it helps to have a starting point and a template for the project. We hope to provide you exactly that in the subsequent chapters.

With that said, let's kick off your plan!

CHAPTER 1 WORKSHEETS

Get your arms around some of the issues by trying the following exercises.

WORKSHEET No. 1

List the ten most critical systems in use in your organization by business impact.

Consult executive management if necessary. Remember to measure in terms of the four items covered in Chapter 1 and Chapter 2: (1) lost sales, (2) lost market share, (3) lost production, and (4) lost public image or customer confidence.

List the systems here by name:

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____
9. _____
10. _____

WORKSHEET No. 2

Taking the ten systems identified in Worksheet 1. List the three most critical supporting technologies for each (example: LAN, Mainframe, 800#, etc.).

BUSINESS SYSTEM	*TECHNOLOGY*
1.	A. B. C.
2.	A. B. C.
3.	A. B. C.
4.	A. B. C.
5.	A. B. C.
6	A. B. C.
7.	A. B. C.
8.	A. B. C.
9.	A. B. C.
10.	A. B. C.

WORKSHEET No. 3

List the ten most probable natural disasters for your municipality or geographical area (e.g., hurricane, tornado, earthquake).

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____
9. _____
10. _____

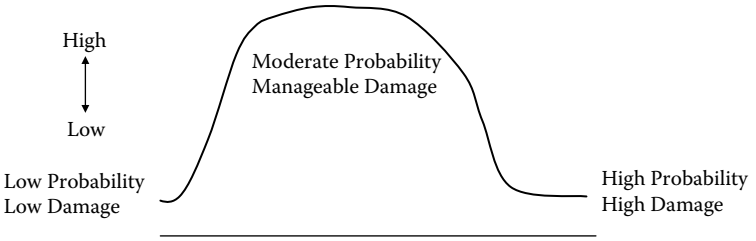
WORKSHEET No. 4

Of the possible natural disasters listed previously, rate each by likely occurrence, from 1 to 5, with 5 being the most probable. For example:

1 = Every 100 years
2 = Every 20 years
3 = Every 5 years
4 = Annually
5 = Multiple times annually

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____
9. _____
10. _____

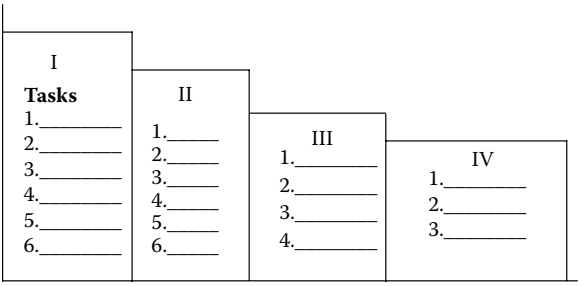
WORKSHEET No. 5



Rate your vulnerability to human-caused disasters such as sabotage or programming errors. You may need to include building security or change control departments to get a reliable number. Rate 1 as the lowest vulnerability and 5 as the highest. Use the "top ten" business systems and supporting technology (from Worksheets 1 and 2) to aid your analysis.

BUSINESS SYSTEM (FROM WS __)	*TECHNOLOGY (FROM WS __)*	*CRITICAL RATING (1 TO 5, 5 HIGHEST)*
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		

WORKSHEET No. 6



1.	2.	3.
4.	5.	6.
7.	8.	9.
10.		

A. List the "top ten" vulnerabilities above, then chart them in the bell curve above in order of significance.
B. Print this page and turn it over to an administrative support person to create a PowerPoint slide for your executive presentation. See Chapter 2 for more details.

WORKSHEET No. 7

Scoping the Project

1. TIME IN DAYS _____	TIME IN DAYS _____	TIME IN DAYS _____	TIME IN DAYS _____
2. ESTIMATED COST $_____	ESTIMATED COST $_____	ESTIMATED COST $_____	ESTIMATED COST $_____

A. Use the diagram above to chart out the "100,000-ft view" of your disaster recovery project plan.
B. Print this page and turn it over to an administrative support person to create a PowerPoint slide for your executive presentation. See Chapter 2 for more details.

WORKSHEET No. 8

Preliminary Business Impact Analysis

BUSINESS SYSTEM	*DAILY REVENUE*
1.	$ _____
2.	$ _____
3.	$ _____
4.	$ _____
5.	$ _____
6.	$ _____
7.	$ _____
8.	$ _____
9.	$ _____
10.	$ _____

Take the "top ten" critical systems identified in Worksheet 1 and fill in the estimated daily lost revenue if that system becomes inoperable. Remember to get the input of the following people in your analysis: vice presidents of Sales, Marketing, and Operations. After you are comfortable with a figure, be sure to filter it through one final executive, the VP of Finance or Corporate Controller, and then print this page and turn it over to an administrative support person to create a PowerPoint slide for your executive presentation. See Chapter 2 for more details.

WORKSHEET No. 9

Preliminary Business Impact Analysis

List available consultants and range of their hourly compensation. Estimate the number of hours and total cost for each project phase. Use this worksheet to flesh out Worksheet 1 with the four phases of your project.

CONSULTANT	*COST/HOUR*	*PROJECT PHASE*	*NUMBER OF HOURS*	*TOTAL COST*	*REMARKS*
1.					
2.					
3.					
4.					
5.					

WORKSHEET No. 10

Preliminary Business Impact Analysis

List all departmental managers and functional heads who will have to be interviewed before the executive presentation.

NAME	*DEPT/FUNCTION*	*NUMBER*	*REMARKS*
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			

Comments

_____

_____

_____

Chapter 2

Understanding Business Impact Analysis

Frank W. Gesinski and Leo A. Wrobel

Contents

What Is a Business Impact Analysis (BIA)?.....23
Data Collection and Verification 31
Report.....32
Additional Observations on Using the BIA to Pitch Management.....36
Using Meaningful Data to Get Your Plan Funded..... 40
Tabletop Exercise 40
Introduction 40
Planning the Exercise.....41
Chapter 2 Worksheets.....47

What Is a Business Impact Analysis (BIA)?

No, BIA is not a branch of the federal government that does covert security work, nor is it a medical procedure that you're too embarrassed to mention to your family or friends. A BIA, or Business Impact Analysis, as the term implies, is an examination and determination of the impact of a catastrophe on a particular company or organization. Another way of putting it is that a BIA is the process of analyzing all business and production functions and the effect that a specific disaster may have upon them.

The BIA process can include, but is not limited to:

- Reviewing business and production processes and identifying interdependencies
- Assessing the impacts of an extended business or production outage
- Determining the time-sensitive processes, functions, groups/departments, and work areas
- Identifying the systems, data, and telecommunications supporting time-sensitive processes, functions, and groups/departments
- Determining the recovery requirements for groups/departments
- Identifying the recovery time objective (RTO) — critical recovery time or the maximum amount of time that a system, application, or group/department can be out of service without severely affecting the company's or organization's revenue flow, production, or services
- Estimating how much revenue and productivity would be lost if your organization were unable to conduct business for a prolonged time frame
- Identifying which critical business papers and electronic files are backed up regularly, and where the backups are kept

A BIA also determines the impact of a disaster on various facets of a company or organization, including financial, operational, legal, regulatory, partner, customer, and employee morale.

Most business continuity professionals have their own unique method of doing a BIA, unless they used a canned, third-party software package, in which case that package determines how the BIA will be carried out. Nevertheless, whether you use a software package or have your own way of doing a BIA, all of these methods make use of the same general principles and the same data or a subset of it.

Other factors that affect how you do a BIA are the time and budget limitations. If you have the luxury of sufficient time and budget, you can do a very detailed analysis, which is preferable. However, if either or both of these factors are limited, then it is possible to do a "short" or "limited" BIA, collecting only the most critical data to get the necessary information to obtain results that are as accurate as possible.

Depending on the scope of the project, you may want or need to do a Risk Assessment (R/A) before doing the BIA. However, if time, funds, or scope are limited, the BIA Questionnaire can include questions that help to identify the critical risks. (See Figure 2.1.)

If you came to work in the morning and couldn't get in the building, couldn't access any of your paper or electronic files — not even from a PC located elsewhere — for several days or weeks, could your company or organization still stay in business?

One of the factors that needs to be considered when doing a BIA is how a company or organization could continue to do business if none of the employees or management could enter the offices or data center after a disaster. Such a calamity

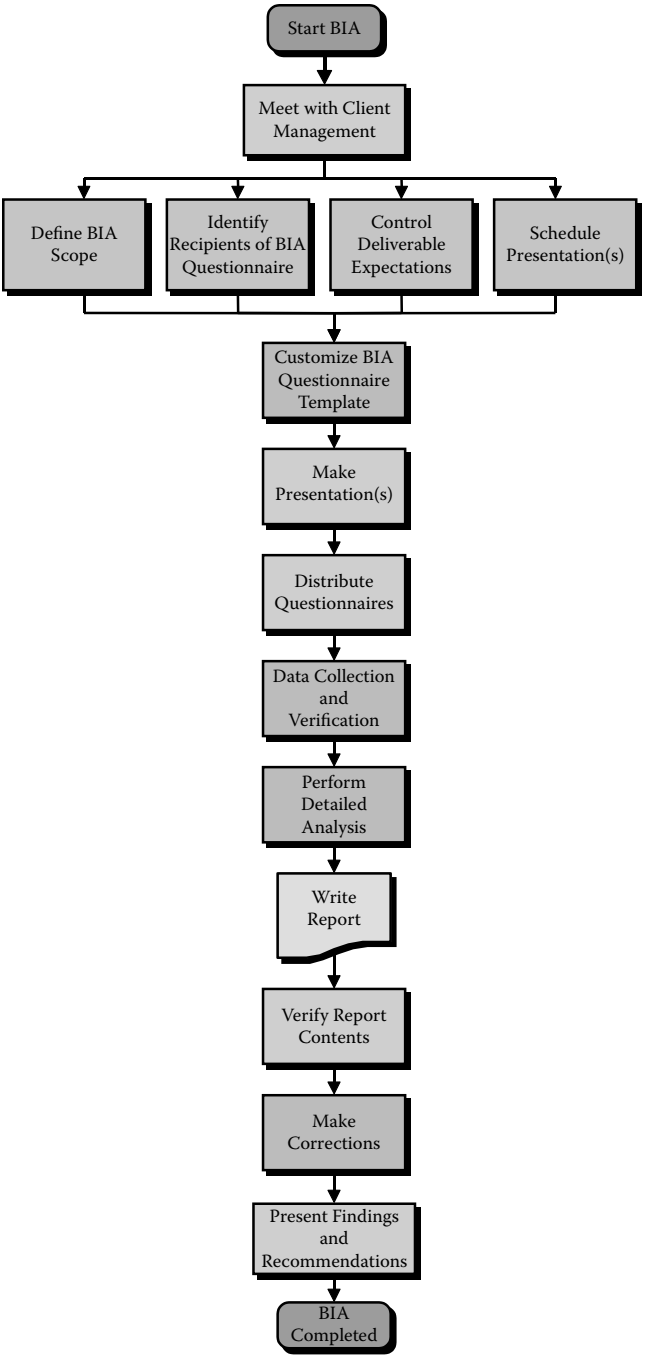


Figure 2.1 Flowchart of a typical Business Impact Analysis.

could also preclude accessing any company information or data, be it via telephone, LAN/WAN, dial-up, etc.

Nearly 400 small businesses never recovered from the Oklahoma City bombing.

Although much of the following material is directed at BCP consultants, the principles presented are equally applicable to in-house personnel who may have been delegated to do the recovery planning for a company or organization.

Initial Planning Meeting with Client

Once a contract has been signed, an initial meeting with the hiring client management should be held to do the following:

- Tell the client what kind of information you will be collecting with the BIA questionnaire.
- Identify the personnel who will receive and fill out the questionnaire.
- Schedule one or more presentations to the identified personnel.

Define BIA Scope

As with all projects, you must determine the scope of the BIA. This can be done by meeting with the appropriate management initially to determine their expectations for the outcome of the BIA. At this point, it is imperative that you set the client's expectations, telling what deliverables they will and will not get from the BIA.

Identify Recipients of BIA Questionnaire

In the initial meeting with management, you need to mutually agree on who the recipients of the BIA questionnaire will be. In most cases, they will be the managers, project leads, or heads of departments, as they are generally more knowledgeable about the wide scope of activities in their area. They may not be able to answer all of the questions, but they can delegate others to answer some of the more technical questions regarding budget, communications, computers, etc.

Control Deliverable Expectations

If the people you are dealing with have never participated in conducting a BIA, they may have some unreasonable expectations as to the deliverables you will provide. As part of the agenda for this meeting, you should set aside several minutes to review in some detail what the BIA report will contain and, more importantly, what it will not contain.

Schedule Presentations

Finally, the client should schedule (or arrange to schedule) the dates, times, and places where you will make your presentations to the questionnaire recipients. As with the deliverable expectations, you should let the client know what you will cover. At this time you should also arrange for any equipment you might need to make the presentations, such as projectors, PCs, screens, handouts, etc.

Questionnaire

Once the scope of the BIA has been determined from the client meeting, you must modify the BIA questionnaire template accordingly.

The type of information you are going to collect will vary from project to project, depending on such things as the size of the company or organization, the amount of time you have to complete the BIA, how much access you have to the people answering the questionnaires, etc.

The information that the questionnaire gathers may include, but is not necessarily limited to:

- Accounts Receivable (A/R) standards
- Accumulation of nonprocessed transactions
- Business and technical impacts
- Business and technical recovery requirements
- Bypass plans and procedures
- General concerns of a major business disruption
- Impacts on client's customers
- Interactions between client and customers
- Interactions between client and suppliers
- Location and type of off-site storage
- Methods and frequency of backing up data, computer programs, and operating systems
- Monetary effects of a major business interruption
- Operating expenses incurred during an outage
- Production and company processes and procedures
- Production computer programs
- Legal consequences of a major business interruption
- Regulatory consequences of a major business interruption

Questionnaire Format

The BIA questionnaire can be in hardcopy or softcopy, depending on the client and the situation. It's also possible to use both formats, depending on the recipient and resources available. An electronic copy is easier to handle because, generally

speaking, you won't have to transcribe (or have transcribed) the answers into your database.

Personnel

Normally, a company or organization's critical employees would be expected to execute a recovery, be it on-site or at an off-site recovery center. However, keep in mind that in an area-wide disaster, employees would give their homes and families priority over their work. They might refuse to go to work to do the recovery. In this case, alternate personnel would need to be available and identified in the Recovery Plan.

Alternatively, if a company or organization contracts with a backup site, the contract can provide for alternate personnel supplied by the backup site during recovery. Obviously, recovery center personnel would have to periodically get updated training to have the knowledge to perform the recovery for a client who could not supply personnel.

The BIA questionnaire should include information on all personnel needed during the recovery, including management, salaried and hourly personnel, and support staffs. Keep in mind that all may not be needed the first few days, so the questionnaire should specify how many people are needed the first day of recovery, the second day, etc.

Equipment

To perform a company or organization recovery, damaged or destroyed equipment — computers, fax machines, telephones, voice mail hardware, filing cabinets, desks, chairs, copiers, PCs, laptops, printers, forms, etc. — would need to be replaced. Even when such services are contracted for ahead of time, the equipment may not be available, installed, and available for use within the time frame required by a company or organization doing a recovery.

Another solution is to contract with a company or organization backup site. For a subscription fee, this site could provide the facilities, equipment, and personnel to resume business operations on short notice for the affected company or organization. This approach is usually much more economical than mirroring facilities and equipment, or any other approach.

Voice Communications

As we all know, voice communications is one of the most critical elements of company or organizational operation. A disaster could disrupt voice communications. During an area-wide disaster, not only telephones but also cell phones are quite

often useless because the phone networks rapidly become saturated, and they can only handle a certain number of calls at any one time.

Data Communications

The same principles that apply to voice communications recovery also apply to data communications recovery. LAN/WAN recovery can, potentially, be especially difficult and time-consuming without specialized expertise to supervise and execute it.

Facility

For a company or organization that has one facility, the Recovery Plan must provide some means of recovery if that facility is destroyed or if, for any reason, no one can enter it for several days or weeks. Most people are unaware that most municipal fire departments have the authority to quarantine a building or facility during an emergency. For example, if a hazardous material (HazMat) spill were to occur just outside a company or organization's facility, the fire department could prevent anyone from entering that structure for several hours, days, or even weeks. This would make it very difficult for a company or organization to continue, resume, or recover their business operations in a reasonable amount of time unless they moved to a recovery site.

Data Backups

Data is critical to the recovery of any computerized business operation. It is the one element that usually cannot be recreated if it is lost. Data can be softcopy (electronic) or hardcopy (paper). Electronic data can include operating systems, computer programs (applications), word processing files, spreadsheets, databases, etc. Some experts exclude operating systems and applications from this classification, but include only files created by the users.

Backups can be taken several times a day, a week, or a month, depending on the production volume and the nature of the organization's business, but especially depending on how long the company could afford to be nonproductive.

Backups are generally categorized as baseline or incremental. Baseline backups involve transferring critical files — in their entirety — to tape, disk, or to another computer. Incremental backups involve transferring only those files that have changed since the last baseline or incremental backup was taken. As you can imagine, incremental backups take less time to do, thereby saving valuable computer and personnel time as well as storage space.

Off-Site Storage

In addition to baseline and incremental backups, data backups fall into two other categories: those kept in or near the computer room for rapid user data recovery, and those kept off-site, to be used to recover from a serious problem.

Backups kept off-site should be stored in a secure location that is sufficiently distant from the production facility so that, in the event of a major, area-wide catastrophe, both sites will not be wiped out. One rule of thumb used for many years by business continuity professionals is that the backup storage site should be a minimum of 7 to 10 miles from the processing site. However, although this is a general rule of thumb, there are geographical locations where this recommended distance would not be acceptable. For example, in Tornado Alley, or along the Florida coast.

Computer Application Programs

Some software vendors encode their proprietary software so that it will run on one particular machine — identified uniquely, usually by serial number — and not on any other. If a company or organization were trying to recover on an identical but different machine, this software would not function until the vendor supplied a key or some other means of "unlocking" the software to run on the recovery machine. Arrangements need to be made with the software vendor ahead of time, and documented in the Recovery Plan.

Workaround Plans and Procedures

As part of the BIA, the questionnaire should uncover what workaround and recovery plans already exist, so that they can be incorporated into the Business Continuity Plan or Disaster Recovery Plan that would be developed once the BIA has been completed.

Make Presentations

The purpose of the presentations is threefold:

- Convey what a BIA accomplishes and how it fits within the scope of business continuity planning.
- Review the BIA questionnaire in some detail to let the personnel know what data they will need to supply, and precisely what kind of data you expect to get from them. Be certain to set a target date by which all the filled-out questionnaires have to be turned in.
- Ensure that the personnel understand that, depending on the size of the organization or company, they may not be able to answer all the questions, but

may have to get the necessary data from subject matter experts (SMEs) or other management in their organization.

Distributing the Questionnaires

If the questionnaires to be distributed are in hardcopy form, they can be distributed at the end of your presentation. We do not recommend distributing the questionnaires at the beginning or during the presentation, because some people in the audience may be distracted and not pay attention to the important details.

If the questionnaires are in softcopy, they can be e-mailed to the recipients soon after your presentation.

Another method, which would take quite a bit of preparation time up front (unless you are using a third-party software package), would be to have the participants enter their data into a Web site that you have constructed, or into a program designed to collect the BIA data from multiple users.

You may encounter some cases where you will have to meet one on one with recipients who feel that they cannot take the time to fill out the questionnaire. At that meeting, you will go through the questionnaire, having them give you the answers verbally, with you transcribing their responses with pen and pencil, or with a PC or laptop. This approach can be most effective when the organization is small, and so is the scope of the BIA.

Data Collection and Verification

Collection of Data

Once you start receiving the data from the questionnaires, you can start placing it into a database for analysis, if the system you are using does not already do this for you. For hardcopy data, this may involve transcribing into an electronic form. For softcopy, this may involve copying and pasting the data into your database.

What Can You Do?

- Enter responders in a contest, such as selecting one for a free lunch or gift certificate
- Follow up with calls (time-consuming)
- Place reminders in company papers or newsletter

Answer Questions

Quite often, when recipients are filling out the questionnaire, they may have questions regarding what specific kind of data they need to supply. You need to make yourself available on a regular and consistent basis to answer these questions, be they in person, by phone, or by e-mail.

Verify Data and Correct

As the questionnaire responses roll in, the data must be reviewed for inaccuracies, discrepancies, and data not supplied. You can then contact the recipient to clarify any problems you encounter in the data, or you may find it necessary to schedule an interview to clarify the data supplied.

Do Preliminary Analysis

While you are gathering the data, some preliminary analysis can be made, and notes made for use in the detailed analysis.

Perform Detailed Analysis

Once all the data has been received from all the participants, the detailed analysis of the BIA data can be made. We strongly advocate the use of spreadsheets and charts, both for analysis and for inclusion in the final report. Executives especially love charts because they can get a lot of information in one glance.

Report

Contents

We recommend the following outline:

- Management summary
- Assumptions
- Findings
- Recommendations
- Appendices

Management Summary

As is typical in a technical report, this section should be one to two pages long, highlighting the principal findings and recommendations from the full report. Because of the length of this section, charts and graphs should be kept to a minimum, or not used at all. The management summary should contain enough information to give management reading it a good idea of the full contents of the report, and what actions need to be taken. The reader can then go to the full report to get any details that were not included in the summary.

It is always good to put the financial findings and recommendations near the beginning of this section, together with a small table to illustrate them, because financial impacts are nearly always management's primary concern. An example follows.

Management Summary

Priority	*Financial Impact after One Day*	*Financial Impact after One Month*	*Critical Function*
1	$100,000 or more	$10 million or more	Yes
2	$1 to $99,999	$100,000 to $9.99 million	No
3	None	None to $99,999	No

Recovery Priority Classification

Assumptions

This is a very important section. You need to list all assumptions made in the analysis involved in preparing the report, such as: "The information and data returned in the BIA Questionnaire is accurate and complete," or "All dollars used in analyzing Canadian accounting financials were converted from Canadian to U.S. dollars."

Findings

As the name implies, this section should contain all the information gleaned from the analysis of the data supplied. We recommend subdividing this section into the various categories used in the BIA questionnaire. Leave all recommendations based on these findings for the next section. A sample finding follows:

> The financial impact to XYZ Company after a disaster approximately doubles for the first three days after the disaster, increases significantly after one week of being out of service, and even more significantly after two weeks. (See Figure 2.2.)

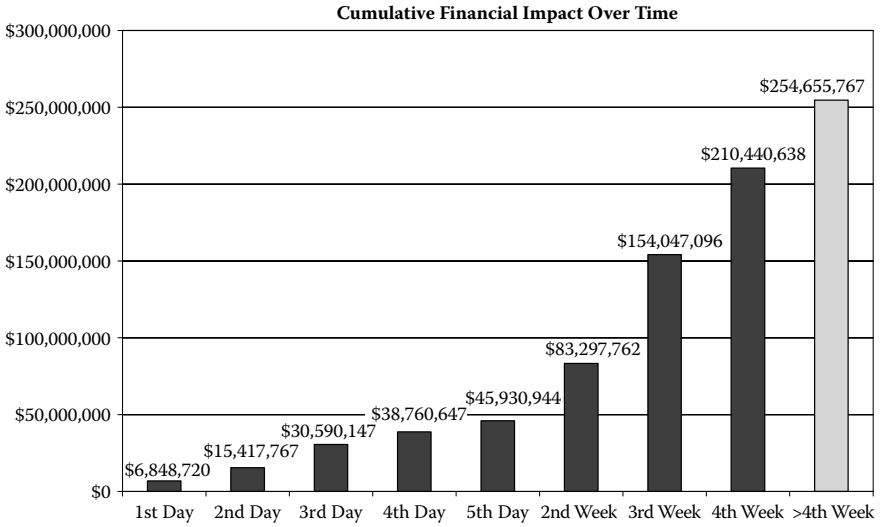


Figure 2.2 Findings.

Recommendations

Here you can tell the client's management all your recommendations to remedy any problems you have uncovered in the analysis. Most — but not all — of these recommendations will apply to the development of a Business Continuity Plan or Disaster Recovery Plan. Charts, tables, and diagrams should be liberally used here for greater impact, particularly in the findings. (See Figure 2.3.)

Appendices

The appendix or appendices should contain any data too detailed to include in the body of the report, and can contain copies of all the data collected from the questionnaires. That way, if someone reading the report questions any findings, they can verify that the data was accurately interpreted.

Writing the Report

A BIA report will help you identify your client's critical computer and business operations, business processes, departments, and divisions. This report will pinpoint where they are most vulnerable if something should happen to their buildings, facilities, or equipment.

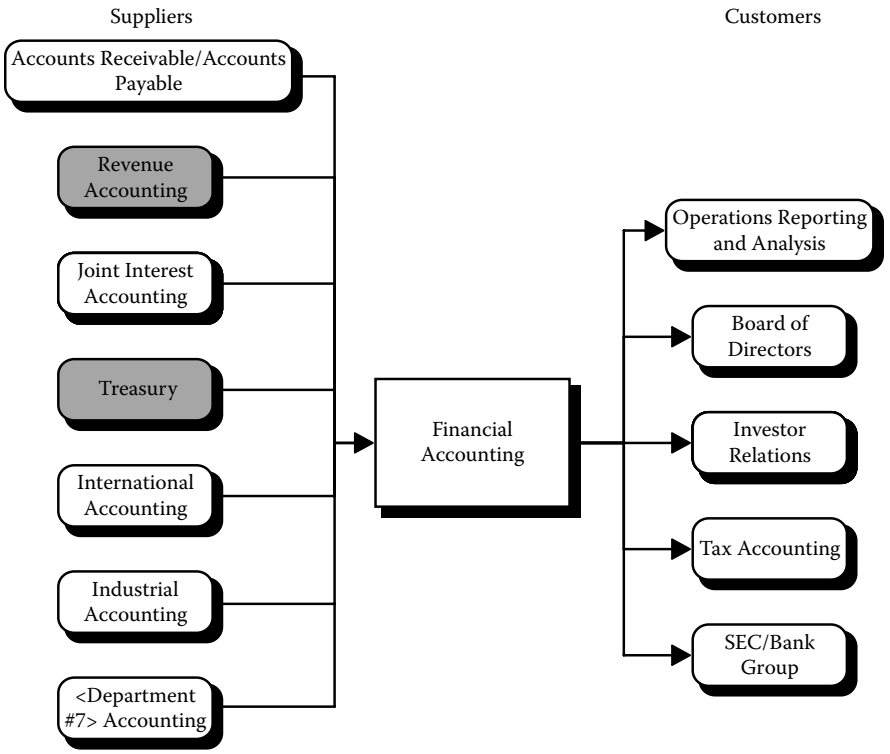


Figure 2.3 Sample dependency flowchart.

Verify Report Contents with Client

Once you have completed the draft of the report, you should have the hiring client management review your work, and provide any corrections, changes, or deletions they feel are necessary. You can then incorporate the changes to produce the final document, and have sufficient copies made for handing out at the final presentation.

Final Presentation

Present Findings and Recommendations

Once the final document has been completed, it is time to produce another presentation. This one will contain your findings and recommendations, as uncovered by your analysis of the data provided in the responses to the BIA questionnaire. Once completed, enough copies of both the final presentation and the final report should be made for distribution at the presentation. Usually it is a good idea to have as many copies of the presentation as there will be attendees. But, again, we

recommend that you not hand these out until the end of the presentation. You probably will have to make a limited number of copies of the final report, as determined by client management. Sometimes, clients prefer to receive softcopies of the report so they can print the hardcopies themselves.

Quite often, the attendees at this presentation include the involved vice president, his or her direct reports, and any other management or technical personnel directly involved in the project or requested to be present by management.

This presentation should be limited to a 1-hr maximum, and it should highlight the major findings and recommendations in your BIA report. In most cases, management's major concerns are financial, so you should devote a significant amount of time in your presentation to cover this. You should also set aside enough time to answer questions that are certain to arise.

BIA Completed

Now that the project is over, you can go on that vacation in the Bahamas that you so richly deserve.

Additional Observations on Using the BIA to Pitch Management

While Frank is enjoying himself in the Bahamas, let me (Leo) share a few more points as to why the BIA is unquestionably the most important part of your plan. First and foremost is the fact that you will not secure support and funding for an expensive and time-consuming project unless management knows what you are trying to protect.

By the time this book is published, Hurricane Katrina will be a dim memory for many people or at best a "don't let this happen to you" slide in someone's disaster recovery seminar. But will you have a plan in 2009 because of the events of 2008? My experience says "maybe." Barring some cataclysm between now and when this book is published, count on "selling" disaster recovery to be an uphill battle in your organization. I base my somewhat pessimistic assessment on personal experience.

In 1991, I was asked to go to Tel Aviv to teach a seminar on disaster recovery planning based on one of my books. My first reaction was shock. It seemed to me that the Israelis should be teaching me, not the other way around. The prospect of going to the Holy Land was absolutely intriguing to me, so I accepted the assignment.

I arrived only three months after the start of the first Gulf War. The locals told me that if I had arrived only days earlier, they would have given me a gas mask to wear at Ben Gurion Airport. I also met many wonderful friends after my arrival, and for most of them the memory of taping up plastic to create a "safe room" in

their homes (from poison gas attack) was clearly a very recent memory. After going to work, I was greeted by a number of highly educated and technically savvy Israeli nationals who believed the recent war was their ticket to a most profitable seminar. After all, what could be more compelling to the Israeli financial community and all the banks that operate in Tel Aviv than a war? Even after 9/11 we Americans are relative lightweights in comparison to what these folks have had to endure. Most of the people I met actually saw the Scud missiles come down. I got to see where they came down.

Contrary to what was being reported on CNN and other media — that the missiles were falling into the desert or being shot down by Patriot missiles — I saw three missile craters. They all hit center city. One was where an apartment building used to stand. Each crater was undoubtedly a compelling advertisement for contingency planning.

Interestingly enough, however, the people who were hosting this seminar told me that when they telemarketed the seminar, the most common response they got was, "Oh, that will never happen to me!" Ultimately, "only" 44 people signed up for the seminar. I was delighted; that's a pretty good turnout by U.S. standards. The local seminar hosts, however, literally expected hundreds to attend. What does this little story tell you about human nature? What does it tell you about what to expect when you try to "sell" disaster recovery to someone who has not recently been in a war? I suppose it tells you that even the most visible and widespread disasters become almost passé with the passage of only a relatively short time. It was then, when I realized the human aspect of trying to sell disaster recovery in this context, that I realized I had better learn a lot more about selling the concept!

Getting the Plan Funded: What Does Management Need to Know?

When you get right down to it, in order to get funded your management really only needs to know:

What can happen?
What is the percent probability that it can happen?
What does it cost when it happens? (productivity and sales)
What does it cost to make the problem go away?

Why Will Management Believe a Consultant But Not You?

Let me answer this question by explaining it in a somewhat novel way:

Question: Where do you get absolutely the best food in the world?
Answer: Generally speaking, it is at mom's house.

Go with me on this one, I intend to make a point.

I grew up in a large Polish/Italian family. (I guess that means I will make you an offer that I don't understand.) The food was good, and there was plenty of it. In fact, there was never any question that it was good. Word spread, and after a while most of my friends discovered that Saturday night was pizza night at the Wrobels and they all came over … often.

Having established that point, let me ask another question:

Question: Where do you go to eat something that nobody in his right mind would normally eat?
Answer: A French restaurant.

I have eaten some pretty bizarre entrees in French restaurants that I would never have consciously chosen to buy at my local supermarket. But they were displayed with such exquisite sauces and elegant presentations that I really enjoyed eating them very much. Also, considering the fact that a meal for two was $250, I had darn well better have enjoyed it.

So what does this analogy mean in real life?

1. First, the food is so good at your mom's house because you have had a long-standing relationship with your mom. In other words, you know it is good because there is a long history of good food involved, and you have first-hand experience.
2. If I can pick on Mr. Gesinski for a moment, Frank might not be so inclined to eat at my mom's house, because he would not have the same first-hand experience. Both of us could probably agree, however, on the French restaurant; after all, if it's so expensive, it has to be good. This is, in a strange way, how management acts.
3. In the case of disaster recovery, you are effectively in the role of mom. You are a great cook, and are more than ready to dish up something healthy and good for the organization — a BIA and a Disaster Recovery Plan.
4. Management does not have the "trust" relationship with you yet. They are reluctant to believe you know how to cook up a plan — in much the same manner that Frank may not want to eat at my mom's house.
5. So, management will instead opt for the equivalent of the French restaurant. They will hire a $350-per-hour consultant to tell him or her things that you already know. Similar to the French restaurant, the consultant is so expensive that he had better be good.

The manner in which the French restaurant — or the high-priced consultant — justifies earning the big bucks is the same. They are both experts at presentation.

It is safe to say, however, that the extra expense of the consultant is not justified if your company has good cooks on staff; however, the company just does not trust them. This is why you must convince management that you are a master chef. You do that in the management presentation.

"Cooking Up" a Compelling Management Presentation

Even after the recent disasters, trying to "sell" disaster recovery planning to management is as challenging as it ever was. Granted, from time to time there are opportunities to advance the cause in the period immediately after a disaster hits. Even these catastrophes are fleeting, as people forget about them quickly. Companies quickly get back to business as usual after these events, forgetting what happened or what they were going to do about it. For example, right after Katrina and Rita, management was receptive to the idea of Disaster Recovery Plans, especially when it came to flooding. It was fairly easy to get a meeting "upstairs" to discuss the topic. Except for the remembrance of the anniversary of the events, have you seen the interest begin to wane, especially in the mainline media, in the months following the disaster? This is typical of human nature, and it is illustrative of why it is important to execute when the concept of Business Resumption Planning is still a focus of attention.

Even at times of relatively high interest, management is reticent to fund the effort and to commit financial or personnel resources. This leaves technologists like us to use a "guerrilla" approach that primarily involves surfing the Web and searching libraries for inexpensive solutions. It also involves tackling the project largely as "kitchen table" work in the evenings because your regular daily responsibilities do not go away, and God forbid, this project might involve hiring staff. So how does one convince management to authorize hiring and other expenses to get the job done? There are a few proven tactics you can employ to do this.

Believe it or not, management is not bashful about spending money. I know, you are probably going to quote me that old Three Stooges routine:

Moe: If you had a dollar, and your father gave you a dollar, how much would you have?"
Larry: One dollar.
Moe: You don't know your arithmetic.
Larry: You don't know my father.

Change the word "father" in the joke to "manager" or "boss," and I think you will see the similarity.

Notwithstanding the levity, it is possible to get your disaster recovery planning effort funded. If you know how to speak in terms that management uses (they are not going to learn your technical terms, sorry), you can use the recent rash of

megadisasters to advance your disaster recovery plan and get it funded. In fact, you can use the same concept of speaking to management in terms they understand to justify most any capital outlay. Let's look at how to, and how not to, ask the boss for money.

Using Meaningful Data to Get Your Plan Funded

In the following chapter we will present an actual, and successful, executive presentation for a $100 million bank. The bank, Deep Pockets Bank, or DPB, has been obviously renamed for this publication. The presentation makes note of highly visible and expensive business issues that management will understand, such as:

- The bank takes a huge financial hit every time its fraud system is down.
- It recognizes the fact that the bank has a parent company, and that the parent company has a lower "pain threshold" when it comes to disasters.
- It acknowledges a high dependence on outside providers, meaning that when the network that connects to these providers is down, business stops.
- It addresses business issues that will be meaningful to management, not technical issues that management will not understand.

Follow along in the next chapter and, while you read, think about how you can pull the business issues for your organization into a compelling management presentation that will get your plan funded. Use our cookbook to prove to your management that, when it comes to disaster recovery, you are the master chef.

TABLETOP EXERCISE

Introduction

A tabletop exercise is a realistic simulation of a disaster, based on a detailed scenario. It is, as the name implies, usually carried out around a table or tables. It involves a minimum number of personnel, those critical to everyday operations — management and technical experts.

The main goal of a tabletop exercise is to exercise a Business Continuity or Disaster Recovery Plan with minimum disruption to a company's daily functions, because the time of a relatively small number of critical personnel is involved for half a day or less. It is meant to train critical personnel so that, if a real disaster occurs, they would already have experience in executing a Continuity or Recovery Plan.

One or more tabletop exercises are usually held before a mock recovery exercise so that, besides training key personnel, errors and omissions in the recovery

plan can be remedied, thereby using personnel and management time much more efficiently.

Depending on the number of participants, a tabletop exercise can vary from relatively informal to formal. An informal exercise involves less paperwork, with much of the communication being verbal during the actual exercise. When more personnel are involved, particularly management-level personnel, it is a good idea to provide detailed documentation — particularly regarding the scenario — both before and during the exercise.

This section is not intended to be comprehensive, but is intended to cover most of the important elements necessary in planning and carrying out a tabletop exercise. Most business continuity professionals will have other areas that they feel are important to add to what we include here.

Planning the Exercise

Management Agreement

Before planning the details of the exercise, it is very important that you clearly delineate for management its scope, objectives, and deliverables and get their agreement. Make certain they understand that key personnel will be tied up for up to half a day for the exercise. You want to make sure that they get what they want for their money.

Schedule Exercise

You should schedule a half-day or less for the exercise, and schedule it sufficiently ahead of time so that the participants can fit it into their busy schedules.

Identify Participants

Facilitator

Normally, the person responsible for business continuity planning acts as the facilitator of the exercise. However, as an option, you can appoint another knowledgeable person with the appropriate background to be the facilitator.

The facilitator's responsibilities include the following:

- Ensuring that all participants understand their role in the exercise and have sufficient information to perform their role.
- Making certain that the exercise starts on time.
- Announcing when the exercise is terminated.
- Conveying the exercise objectives to the participants.

- Ensuring that the exercise sticks to the predefined objectives, and does not deviate from them.
- Remaining impartial.
- Guiding the proceedings toward the objectives.
- Asking questions.
- Being knowledgeable about the details of the exercise, and having the appropriate experience and expertise, including being aware of relevant legislation.
- Ensuring that the scribe documents everyone present, and all problems and important issues left uncovered.

Scribe

Besides the facilitator and the participants, it is very important that you identify a scribe to document all the critical information identified during the exercise. As well as documenting all important issues such as injuries, environmental damage, property damage, etc., the scribe needs to record all details of problems encountered. See Figure 2.4 on p. 47.

Participants

The people you pick to participate in the exercise will normally be management and SMEs (subject matter experts) because, during an actual recovery, they would be the ones who would perform and supervise the actual recovery operation. These would include key personnel involved in executing critical business processes, and supervisory or management personnel with direct responsibility for critical business functions.

It is often said in the business continuity profession that upper management should be placed in a separate room from the EOC (Emergency Operations Center), because they tend to want to take charge and wind up hindering rather than aiding the recovery. After all, it is the day-to-day workers who know and understand the intricacies of performing the recovery, whereas management does not normally get involved in daily operations, unless the company or organization is very small.

The number of participants will determine how large a room you will need. Once again, be sure to allow plenty of time before the exercise so that a room of the appropriate size is available.

Once the room has been scheduled and the participants have been identified, you will need to send a note or e-mail to all the invited participants, giving them the date, time, duration, and location of the exercise. You should also briefly tell them what will be accomplished. Specify that, if they cannot attend, they must send a knowledgeable substitute. Make it clear that they cannot send a novice or junior employee unfamiliar with day-to-day operations, but a person with the

experience and background to perform and direct their part of the recovery. Also, specify an RSVP and specify the time frame in which they need to accept or specify a substitute. It goes without saying that if no response is received within the time you specify, you must contact them. If any invitees refuse to participate, the next recourse is to go to their management. However, this should not be necessary if you have already gotten management's agreement to the exercise and its objectives.

Observers

You can optionally invite observers to the exercise. Normally, they are supervisors and management personnel who have a vested interest in the exercise. Their role is, as the name implies, to observe the exercise, but not to directly participate in it.

Equipment

Besides scheduling the room, be sure to reserve appropriate equipment needed for the exercise, including:

Projector
PC or laptop
Flip chart
Chalk
Crayons
Conference phone line
Copies of recovery plan
Chairs
Pens and pencils

Scenario

The exercise scenario must — above all — be realistic. Otherwise, the participants will become disinterested at the very onset, and you will lose a great deal of credibility. For this reason, when developing the scenario, it is a good idea to take into your confidence one or two SMEs to suggest credible alternative scenarios, and have them review and confirm the details of the scenario you have decided upon.

Once this has been done, prepare a "scenario document" to hand out at the beginning of the exercise. You may wish to send an e-mail or note to the participants a week or so before the exercise, telling them what, in general, to expect. However, it is critical that you not provide the scenario until the beginning of the actual exercise.

Assumptions

Make certain that you identify all assumptions as part of developing the scenario, and list them in the documentation handed out for the exercise.

Characteristics

Realistic

It is vital that the scenario be realistic. As we said earlier, if it is not, your credibility will be seriously damaged, and there would be a good chance that the participants will lose interest in the exercise and not be fully involved.

Sufficient Resources

As part of the exercise, the participants must determine that sufficient resources — personnel, equipment, etc. — are identified in the recovery plan and can be made available during an actual recovery.

Not Overly Complex

If the scenario is overly complex, the participants could become distracted, and the entire exercise could become bogged down in unnecessary details.

Details

The scenario should include the following details:

Date and time of incident
Weather conditions
Description of incident
Injuries and fatalities, if any
Assumptions

Agenda

A suggested agenda for the exercise:

Introduction
Scenario presentation
Simulation exercise

Evaluation
Common findings
Feedback
Conclusion

Types

Each business continuity professional has his or her own favorite types of tabletop exercises. You will need to determine the type of exercise to do based on such factors as the organization's "exercise experience," the size of the organization, what areas need to have their recovery plans reviewed and updated, how many necessary management personnel and SMEs can be made available for half a day, etc.

Some possible types include:

Surprise
Planned
EOC personnel
Communications

Debriefing

Depending on the scope of the exercise, you may want to hold a debriefing meeting to gather any additional information or opinions from the participants. It may be expeditious to hold the meeting immediately after the exercise, when all the participants are still available. Alternatively, you can hold a separate meeting shortly after the actual exercise.

Exercise Report

As soon as the exercise and the debriefing meeting have been held, the exercise report needs to be written.

Executive Summary

A one- to two-page executive summary should be at the front of the exercise report, briefly describing the problems encountered, their solutions, and recommendations.

#	Problem	Date/Time	Dept./Div.	Person	Resolution

Figure 2.4 Problems encountered.

Problems Encountered

The Problem Report generated during the exercise can be included in the appendix to the report. All significant problems encountered should be described in this section of the report, including how they were or will be resolved.

What Went Right

Although the exercise was conducted to determine and correct problems in the recovery plan and procedures, matters usually go as planned. There should be a section in a report delineating these items.

Recommended Changes

In addition to the problems discovered during the exercise, you will probably discover other changes that need to be made to the Recovery Plan and procedures. Be sure to describe them in this section.

Action Plan

This section should say, "Where we go from here." In other words, you should propose the date and type of the next exercise. If the tabletop exercise went well, you might want to hold a live exercise instead of another tabletop. If the exercise did not go as well as it should have, it was the first such exercise held, or the organization or company is large, you might want to hold one or more additional tabletop exercises.

CHAPTER 2
WORKSHEETS

WORKSHEET No. 1

Business Impact Analysis

The following persons have been identified to receive the Operational and Security Standards questionnaire in Phase II.

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____
9. _____
10. _____
11. _____
12. _____
13. _____
14. _____
15. _____
16. _____
17. _____
18. _____
19. _____
20. _____

WORKSHEET No. 2

Business Impact Analysis

Scope of the BIA: (Put "Top 10" here and remarks below.)

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____
9. _____
10. _____

Remarks

_____

_____

_____

_____

_____

_____

_____

WORKSHEET No. 3

Business Impact Analysis

The following individuals will help develop the Business Impact questionnaire:

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____
9. _____
10. _____

WORKSHEET No. 4

Business Impact Analysis

The following persons will review and tabulate the questionnaires and then serve on a Data Collection and Verification Team to verify results.

1. _____
2. _____
3. _____
4. _____
5. _____

WORKSHEET No. 5

Business Impact Analysis

Other Responsible Personnel

TASK	*NAME*
1. Interview consultant	_____
2. Conduct user interviews	_____
3. Create slides and graphs	_____
4. Make the executive presentation	_____
A. Present findings	_____
B. Make recommendations	_____
C. Secure funding	_____

Remarks

_____

_____

_____

_____

_____

_____

WORKSHEET No. 6

Business Impact Analysis

Business Unit Interview Topics

Check all that apply and assign responsible person.

	Topic	*Responsible Person to Interview*	*Person to Conduct Interview*
	Accounts receivable		
	Business impact (high level)		
	Technical impact (high level)		
	Legal and regulatory (including contracts)		
	Customer service		
	Finance		
	Supplier liaison (e.g., JIT "Just in Time")		
	Corporate travel		
	Banking relations		
	Production		

WORKSHEET No. 7

Business Impact Analysis

Here is a tough one. Keep this form CONFIDENTIAL! List your top ten indispensable technical personnel here and their backup in the event of a disaster that incapacitates them.

Name	*Function*	*Alternative*	*Wireless Telephone Number*
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			

Keep this list only to ten — and confidential.

WORKSHEET No. 8

Business Impact Analysis

List your top ten toll-free numbers by function and in order of importance.

Function–Number

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____
9. _____
10. _____

Remarks

_____

_____

_____

_____

_____

Chapter 3

Selling Management with a Compelling Business Impact Analysis and FMEA (Failure Mode Effects Analysis)

Radi Shourbaji

Contents

Getting the Plan Funded (Executive Commitment) 57
Other Ways to Present Your Data 66
What Is a Failure Mode Effects Analysis? 67
Chapter 3 Worksheets.....73

Getting the Plan Funded (Executive Commitment)

It is a well-known fact that the human attention span is about 90 seconds. In a meeting, if a person does not say something meaningful to the audience in that time frame, eyes and thoughts start to wander. With executives, this span shortens to about 15 seconds as they have an advantage. They can count on someone else to recall or record anything relevant you had to say. If what you present is garbled with unfocused data or confusing technical terms, then your presentation will have lost its value because the executive will tune you out.

This brings us to another problem in such a forum. When asking "permission to plan," you will recall from a previous chapter that there are three answers from the executive that are possible:

A. Yes
B. No
C. Let's study this some more

Now, which do you suppose is the answer most often given? And why do recovery plans take ten years to complete? It's because technical people are not always so good at presenting their needs to management. Sure, technical service persons know exactly what they need, but they go about asking for it all wrong. Consider the following example of a presentation opening.

What Management Does Not Want to Hear

> "Good morning. If you will refer to the 168-page report in front of you, you will see that I am here to alert you to some problems with the LAN switches. The network has been down four times so far this year. For starters, we may need a UPS on each, and media access unit at a cost of $5,000 each, and we would also like to upgrade each LAN switch with Amalgamated Revision 4.12 enhanced power and common logic, and hot standby protection switching. Route diversity on each drop throughout the building is costly, but recommended. Furthermore, … "

By this time, the executive is fingering his Blackberry, doodling on a pad, or looking at the next agenda item while expecting someone else to listen to the presentation. What will be the most likely outcome of the meeting? The answer will not be "yes." He or she does not really understand what you are talking about, only that you *think* you need something. The answer will not be no for essentially the same reason. Management does not want to go on record against whatever it was you were trying to ask for! So what is left? The safe play: Let's study it some more.

Because of a few key mistakes, the presenter does not get his funding; instead, he walks out with a longer list of questions from management than the ones he went into the meeting with. The key point to a successful presentation is this: do not speak to management in technical terms. Use business terms. Management understands business terminology, and it is meaningful to them in a presentation. Let's try again another way:

> "Good morning. Are you aware that Deep Pockets Bank (D.P.B) runs the risk of a $750-per-minute financial hit every time the LAN supporting our fraud monitoring system fails? It has happened four times this year. We have identified several areas of exposure, and would like

> you to help us consider protective alternatives, which can prevent this from happening in the future."

Wow, how's that for an opening. Will that get management's attention? You bet, for approximately ten seconds. That's about how long it takes the CEO's head to look around the table and ask, "Where did that $750 figure come from?" When the shoulders all shrug, the meeting is over. Sure, they will listen to you, but no action will be taken because the figures are in doubt. What answer can you expect? You guessed it. "Let's study this some more." Ever notice how disaster plans often take ten years to complete? This is one reason why.

Think about how long it takes to get a meeting with a CEO or a CIO in your company. If you have to take that much time and trouble, go in ready for action, not predestined for failure. Do your homework first.

The best way to "sell" management is to produce believable loss scenarios, and verify your figures with people the manager holds in confidence. These include Vice Presidents (or the equivalent) of Sales, Marketing, Operations, Engineering, Finance, Legal, and other divisions in position to truly assess the effect of a disaster in terms of revenue. A competent consulting company or the company's internal or external auditors can also help because they are credible to management. You will then need a hard-hitting presentation, preferably with less than five slides. Following is a modest example:

Slide 1

The "Politics" of Planning

Support: YOURSELF
Illuminate: YOUR MANAGEMENT

Slide 2

FOCUS ON DEEP POCKETS BANK CREDIT CARD OPERATIONS

OVERVIEW of Banking Operations

- DPB is a wholly-owned subsidiary of Deep Pockets Insurance Inc.
- 300,000 accounts, mostly MasterCard and Visa
- DPB outsources credit card operations
- Telecommunications dependence for both voice and data is high.
- Long outages (i.e., all day) are unusual, but short outages are frequent.
- The bank is a large VRU (voice response user) using this automated system to answer some 500,000 calls per month. 50% of all credit inquiries are via automated voice response.
- Banking via the Web taking off as preferred customer access medium.
- Observation: With the high dependence on outside providers, when the network is down, business stops.
- How much does an outage cost in:
  - Lost productivity and customer confidence
  - Lost sales and market share

Let's consider the next slides and see:

Slide 3

THE HIGH COST OF EXECUTIVE COMPLAINTS

ISSUES:

Complaints are costly— $300 to $800 in personnel costs to process each.

Complaints damage customer confidence and trust.

Besides all this, we could lose the customer!

DYNAMICS OF DPI vs. DPB

* YEARLY (2004) Gross Revenues of $100 Million–312 Business Days

CONSIDERATIONS:

- 80% of credit card holders are Insurance Company (DPI) Customers
- DPB "hurts" from disaster sooner than DPI
- DPB customer base very intolerant to outages, particularly those that preclude access to funds or cause a bankcard to reject.
- Insurance company customers will wait much longer in a catastrophic outage than bank customers, as shown on the two graph lines above.

NUMBER OF IDLED EMPLOYEES AT BANK IN MAJOR FAILURE: 220

LOADED PERSONNEL COST PER PRODUCTION USER: $14.50/ HR.

LOADED PERSONNEL COST PER KNOWLEDGE USER: $32.50/ HR.

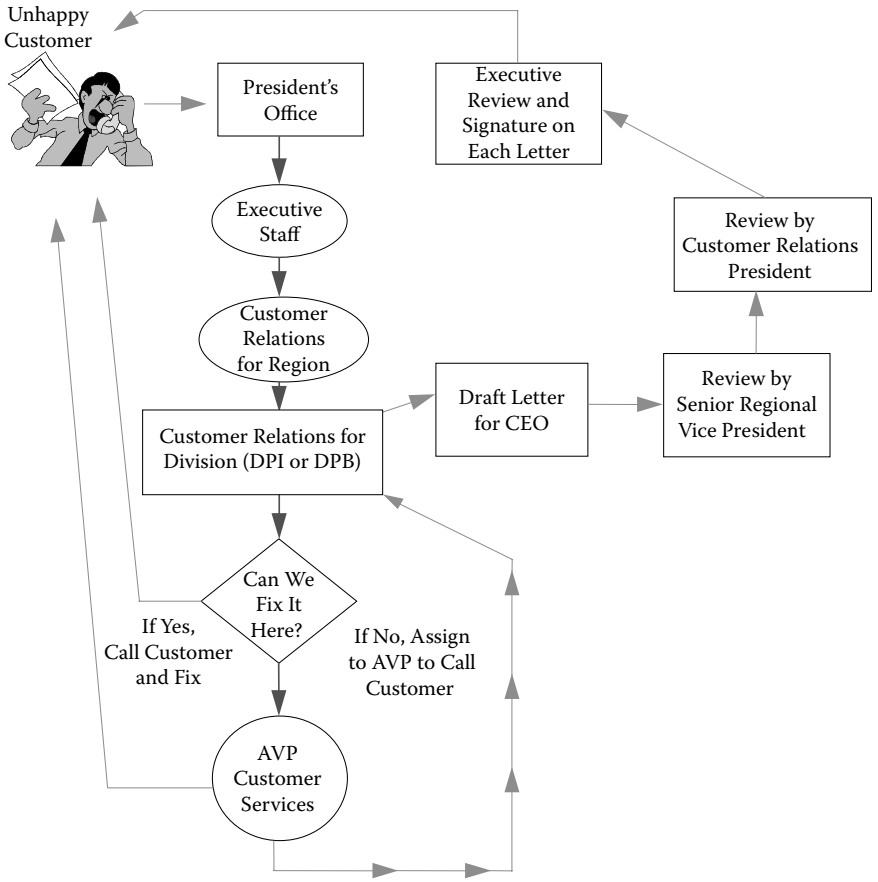


Figure 3.1 The high cost of executive complaints: The cost of each complaint could run $300 to $800 in personnel costs; the complaint could damage customer confidence and trust; the complaint could cause the loss of the customer.

Slide 4

FINANCIAL IMPACT OF LOSS OF CRITICAL CARD FRAUD SYSTEM

Assumes average loss of $75 per minute when fraud system down.

Assumes loss of $750 per minute in hacker attack.

* Figures are CUMULATIVE by day

Slide 5

FOCUS ON DEEP POCKETS BANK
CREDIT CARD FRAUD

LOSSES TO HACKER AND PIRATE ATTACKS

- Typical annual DPB losses to hacker attacks: $1.5–$2.0 million
- Total times DPB hacked last year: 14
- Average duration of hack: 72

TECHNOLOGY RISKS IN FRAUD DETECTION

- Loss of phones (can't call out to investigate suspicious activity)
- Loss of data link to outsourcing company that handles credit cards

POTENTIAL LOSSES TO FRAUD

- Average cost when either phones or data link is down: $75.00/minute
- Average cost of outage if DPB is being hacked at time $100s/minute.
- Average sale to individuals w/counterfeit cards: $10,000–$12,000

RECOMMENDED TECHNOLOGY IMPROVEMENTS

- Total cost of recommended technology improvement: $86,300
- Probability of continued problems without these improvements: 97.75%

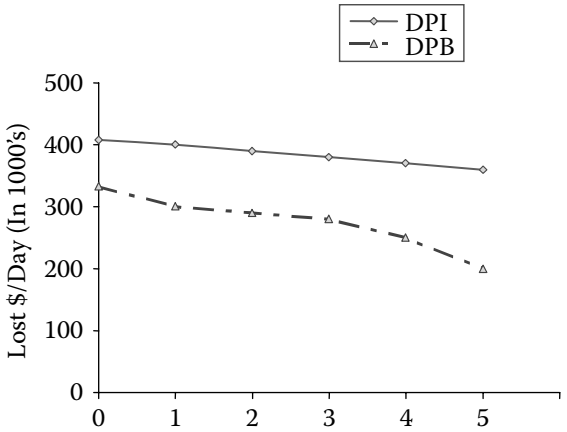


Figure 3.2 Dynamics of DPI versus DPB.

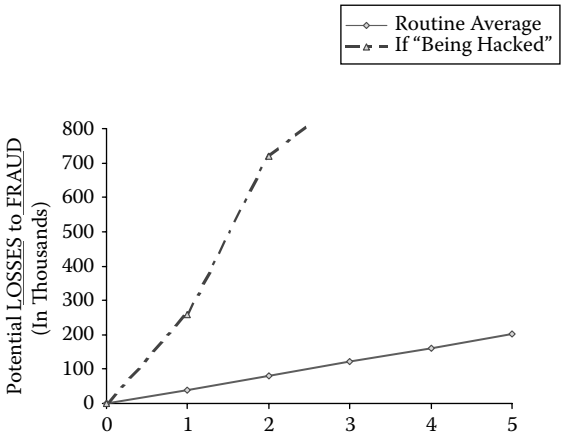


Figure 3.3 Financial impact of loss of critical card fraud system.

Other Ways to Present Your Data

Consider some of the other tools highly paid consultants use to communicate with management. You have just seen some graphs. Another useful tool is to organize your data into an understandable matrix. Here is a modest example:

- Start by setting these up as columns in an Excel spreadsheet for your handout slide. The first "What can happen" column might just as easily be labeled "Event." The event could be "Water in the equipment room."
- Label the second column "Probability." What is the probability that a leak in the equipment room will occur? You can't just dream up a percentage figure

and stay credible, but there are sources where you could get one. For example, the National Fire Prevention Association (NFPA) might have an idea, or consider asking an insurance company, they have actuarial tables for disasters. It is important to not make one up — get one from someone who knows.

- The third should be labeled "Cost when it happens." This is the figure you will want to get from the Vice President of Sales. This person may have an incentive plan based on sales that decides their or her commission. I can bet they would be able to venture a plausible estimate of lost sales.
- Finally, the "What does it cost to make the problem go away?" column. Label it "Remedy" or something like that. That column is yours; after all, you are the technologist and know how to fix the problem.

Now that you understand how to compile a winning funding request for disaster recovery, imagine how the proposal would have gone if you only started with Item 4 — Remedy — and skipped the essential first three items! Yet, this is exactly what technologists do year after year, not because they don't know what they need, but because they don't know how to communicate effectively with management.

RECOMMENDED IMPROVEMENTS

EVENT	*PROBABILITY*	*COST OF OUTAGE PER DAY*	*TIME INDAYS*	*COST OF NEW CAPABILITY*	*FINANCIAL BENEFIT/ PRIORITY*
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
				TOTAL	**$**

What Is a Failure Mode Effects Analysis?

How does one know the probability that a given piece of equipment will fail? After all, management will need to know the probability of a failure in order to commit to funding your effort. They will also need to understand where you got your

figures. In this regard, I found a way to quantify the probability of a catastrophic failure in a piece of equipment or a system that I am especially fond of. It came in part from a conversation with a former Air Force General who was then the CIO of a $75 billion financial services organization. Essentially, everything looking down at Iraq today from orbit was put in by this guy's subordinates when he was still on active duty. He summed it up this way:

> When we send up a military satellite, everything has to be perfect the first time. This is because no one has yet invented a 23,000-mile-long screwdriver to fix it if it is not.

I got the feeling from his tone that this was the voice of experience, but I did not expound on the subject any further. Being a veteran myself, however (a sergeant, not a general), I could only imagine how many rumps would be on the line if someone botched a $100 million satellite launch. Therefore, to enhance its odds of getting it right the first time, the military used a methodology known as FMEA (not to be confused with FEMA) or a Failure Mode Effects Analysis. It goes something like this:

1. Identify every mission-critical component that could fail.
2. Compute or acquire from the manufacturer a mean time between failure (MTBF) for each identified mission-critical component.
3. Combine the failure probabilities into a single mathematical factor that describes the probability of failure of a given system.
4. Use these figures to justify and prioritize expenditures to "harden" equipment rooms, networks, or other facilities.

One can actually adapt this same military FMEA methodology and use it as contingency planners in corporations. We adopted the Internet, right? Here is another military invention we can dust off for commercial use.

Suppose you are tasked with performing a detailed analysis of your equipment room and associated networks. The objective of this analysis is to determine single points of failure, critical components that cause failures to multiple users, and an overall assessment of past performance or incidents. To describe this information, your FMEA will be broken down into three steps:

1. The Problem Identification step: The rule of thumb is to ask, "What can possibly go wrong?" This includes both failure rates of the equipment itself as well as the external factors (heat, water, air, people, etc.) that could affect it.
2. The second step: Assign a Risk Priority Number or RPN value to each of the issues you identified. Pick a number from 1 to 10. The higher the number, the greater the associated risk. (Except in the case of problem resolution, where the higher the number, the better your speed in fixing the problem, as you will see below.)

QUANTIFYING PROBABILITY

1. Where do you get probability data?
   A. Your own history
   B. Experience of others
   C. Research
   D. Trade groups
2. Actuarial tables
3. NFPA (National Fire Prevention Assn.)
4. FEMA, National Weather Service, other agencies

PRESENTING THE PROBABILITY OF A DISASTER TO MANAGEMENT

1. Figures must be substantiated
2. Figures must be relevant to your organization
3. Best to express in % probability
4. Figures must communicate easily
   (Use color, charts, graphs, if possible)
5. Consider conducting a Failure Mode Effects Analysis (FMEA)

3. The third and final component is to quantify the reaction process. This is the "How fast can we fix the problem?" step. (This step is shortened by modifying your company's Operating and Security Standards to moderate the risk and changing the environment to make the selected systems more robust.)

Failure rates are assigned probabilities from actual statistical or historical data accumulated in the past, from manufacturer's data and specifications, or from other sources. For example, you might quote probabilities of a catastrophic equipment room fire from data you acquire from the NFPA or even from your insurance carrier. The three aforementioned factors — severity, frequency, and detection — are then considered and weighted in this process:

Severity is assigned a numerical value from 1 to 10 (the higher the number, the more severe the failure is) based on the probability of an event, and how damaging it would be.

Frequency of the occurrences is similarly assigned a value (the higher the number, the more often it happens).

Detection and repair of the problem is similarly given a number and weighting. In this case, however, the higher the number, the better it is. The higher number means you can respond to and fix the problem faster.

These three factors multiplied together form the RPN. RPNs are used to assist the team in assigning priorities to address or assess higher-priority treatment on specific elements. This is not a qualifier disqualifier but a determination of what can, and ultimately will, go wrong. From there, resources (capital or human) can be assigned to shore up the risks associated with these areas. The issues with the highest RPNs are the areas where your organization is most vulnerable and needs to spend the most time and resources. Consider the following illustrations.

Severity

Description	*Rating*
A single employee is affected	1
A work group is affected	2
An entire floor is affected	4
An entire building is affected	6
An entire campus is affected	8
The entire company is affected	10
Occurrence Level or Frequency	
Daily	10
Weekly	8
Monthly	6
Quarterly	4
Annually	2
Description/Detection	
Detection/resolution (D/R) within 1 hour	2
D/R greater than 1 hr but less than 8 hours	4
D/R greater than 8 but less than 24 hours	6
D/R greater than 24 hours	8
Virtually unrecoverable (e.g., World Trade Center severity)	10

WHAT IS A FMEA?

1. Mankind in 6000 years has never invented a technology that has not failed.
2. Everything has a probability of failing.
3. The space shuttle has a 1 in 100 chance of a disaster every time it goes up. (Source: NASA)
4. In just over 200 shuttle missions, we have regrettably lost two shuttles.
5. Bottom Line: NASA's FMEA figures were correct.

We can compute probabilities in much the same way NASA and the military do.

The single point of failure in this scenario is assumed to be the equipment room; however, many individual components make up this single point of failure. Such factors include not only building environmental conditions mentioned earlier in the article, but a host of other issues related to the equipment itself. Use your knowledge to fill in the blanks. You know your equipment better than anyone else.

Frequency

If the failures continually recur, or manifest themselves on a daily basis, then the critical rating here is the highest.

Detection

Detection works in sharp contrast to occurrences: the easier it is to detect the problem and begin corrective measures, the lower the critical rating. The longer it takes, the higher the rating.

By multiplying the three components, one arrives at an RPN.

$$S \times O \times D = RPN$$

$$10 \times 10 \times 10 = 1000$$

The higher the RPN, the higher the risk associated with a specific component and the higher the value that would be placed on solving the problem. If your equipment room housed many critical components that had very high values of RPN, one would have to show where it could be improved to support the service levels that are expected. This brings us to the final step: standards refinement.

Standards are really there to prevent disasters before they happen in the first place. They will be discussed in greater detail in Chapter 5. Change control and

management is one big consideration because people making improper changes to software can cause so many problems. Change-control issues should therefore be defined in your standards. Often, systems that were well designed in the first place become vulnerable over time as the standards governing their maintenance and operation erode. That's why they should be frequently reviewed and updated. Standards should also include items like those presented earlier in this article, such as standards for water detection or physical access controls. Taken as a whole, standards mean repetitive occurrences of the same problems that can be prevented.

It has been said that if you give an infinite number of monkeys an infinite number of typewriters, one of them will write *War and Peace*. In a way, your FMEA will be like that. Given enough time, every manner of disaster will occur, even a life-threatening event like an asteroid hitting the earth. That does not mean we should spend all of our time planning for our own extinction or a commentary impact on the Earth. This is why weighing the exposures with reliable historical or actuarial data is so important. It allows you to channel your efforts into the projects and improvements that are not just the scariest, but those that really matter most.

ASSESSING PROBABILITY

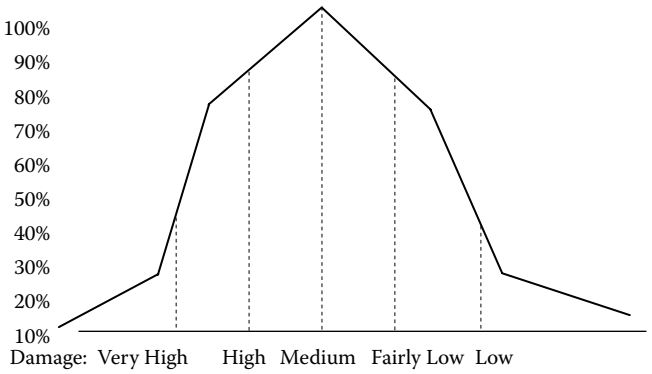


Figure 3.4 Assessing probability.

1. What kinds of events can you imagine fit into each category above?
2. Where would you spend your money?

CHAPTER 3 WORKSHEETS

1. Take a sheet and work up a “fill-in-the-blank” version.
2. Add your own
   - Catchy title
   - Graphics
   - Things to hold management’s attention

FOCUS ON _____

OVERVIEW of _____

- _____
- _____
- _____
- _____
- _____
- _____
- _____
- Observation: _____

How Much Does an Outage Cost in:
Lost Productivity and Customer Confidence
Lost Sales and Market Share

THE HIGH COST OF EXECUTIVE COMPLAINTS

ISSUES:

- _____
- _____
- _____

DYNAMICS OF _____

[Put your graph here]

CONSIDERATIONS:

- _____
- _____
- _____

NUMBER OF _____

_____ **/HR.**

_____ **/HR.**

FINANCIAL IMPACT _____

[Put your graph here]

ASSUMPTIONS

_____

_____

Severity

Description	*Rating*
Occurrence Level or Frequency	
Description/Detection	

Chapter 4

Leveraging Internal Resources to Complete the Plan

Leo A. Wrobel

Contents

Options for Completing the Plan..... 77
Chapter 4 Worksheets.....85

Options for Completing the Plan

It is not always difficult or expensive to accomplish many disaster recovery planning tasks. Sometimes, in fact, resources are right under your nose. Consider all of those old mainframe recovery plans that are still out there. When you look at them, or even at some plans that predate mainframe plans, some interesting facts reveal themselves, chiefly:

- Technology changes so quickly that it is virtually impossible to keep up.
- Planning fundamentals, however, change very little.
- What this means is that although the hardware requirements in mainframe plans are useless, the planning fundamentals are still very useful.

For example, a first-alert procedure that was a good procedure in 1990 might still be good — procedurally, that is — today. Sure, we could augment it now with wireless phones and PDAs (personal digital assistants) but the concepts behind the procedure often stand the test of time. And never mind the 1990-era concepts either.

Sometimes, good procedures are even older. Some components of a successful business resumption plan have not changed in 30 years. Now, before you dismiss this hypothesis out of hand, consider where I was three decades ago. I was in the Air Force in the telecommunications wing. This is where my story begins. The military recovery plans of the mid-to-late 1970s have relevance even today. These plans utilized elaborate telecommunications recovery and restoration plans, and the responsible parties (that was us) practiced them constantly. From that perspective, the planning process itself was extraordinarily advanced for its time. The technology of that time, however, was "stone knives and bear claws" compared to today's technology.

Because the planning process itself has changed very little over the decades, I submit to you that we can borrow from the work of the past and leverage it with the technology of today. In fact, I further submit to you that today's businesses want and need a military level of precision in disaster recovery.

Today's businesses require a level of control and coordination that in the past only the military needed, because minutes of downtime equate to lost dollars. Businesses move billions around every day through every manner of electronic commerce. When money moves this quickly, everything moves quickly. How long, for example, is an acceptable outage for an online stockbroker? The answer today is zero. Yes, you can be assured that if an organization that is highly involved in E-commerce could buy a military level of precision in a disaster, they would.

Taking this line of reasoning a little further, it is generally accepted knowledge that in the opening minutes of a military engagement, the first targets knocked out are command centers and telecommunications hubs. This was not a reassuring notion to me years ago as an Air Force communications technician, because 15 minutes after the Russians got teed off at us, I would have been in the upper atmosphere. Aside from that observation, military planners have long known that you can't respond to any situation without eyes and ears.

Cold War Contingency Planning Practices in Today's Organizations

- 10-minute clearance on international circuits
- Back up circuits and redundant paths—even troops
- "The Big Board"
- Conference calling
- Scripted contingency plans
- The Internet
- Plans for loss of a major telecom hub

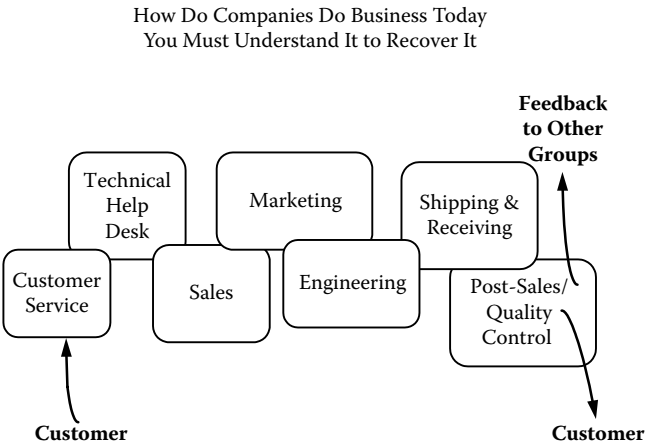


Figure 4.1 Aggressive use of technology with appropriate standards forms a world-class solution for a hypothetical manufacturing company.

Today: Radiological, biological, or EMP threats.

The same holds true for today's organizations with regard to their recovery plans (see Figure 4.1). So, what does this mean for us today, in 2008? It means that many of the activities of the past that were used solely by the military are in demand today by commercial organizations. If you still don't believe me, open your eyes and look around:

In 1977, the military mandated 10-minute clearance time on international circuits. In my former environment, from the time a circuit was reported out of service we had only 10 minutes to have it restored — with 1977 technology. It didn't matter if the circuit went to Hawaii, Guam, the United States, Korea, or the Philippines. (I was in Japan.) It didn't matter if the phone company at the other end was a lackadaisical monopoly, or whether their people spoke English. If a circuit was out more than 10 minutes, you had to answer to someone, and as anyone who is a veteran will attest, you never wanted to answer to someone. But wait, there is more and the story gets even better. After the service was restored in 10 minutes, we had an additional 20 minutes (for a total of 30 minutes) to find the defective component, replace it, and have the circuit restored to the original path. That was regardless of whether the component was in the rack next to you or 9,000 miles away in California. So, how did we do it?

- We accomplished this feat using a lot of "hot lines" and items called "order wires" not unlike the "red phones" you see in the movies. They really have them. For places we worked with all the time, we used "hoot and holler" circuits, where you picked up a phone and just yelled over it for the site that you wanted. (For people too busy to even wait for a ring!) So fast forward to 2008 again. Today's order wires might be Nextel phones where you "get right

through" using a walkie-talkie feature. Furthermore, the user who demands 10 minutes clearance time on an international circuit might just be your company's main call center, which is now in India (see Figure 4.2).

- There are other ideas we can borrow from the past. Who else in 1977, except for Uncle Sam, constructed hardened disaster recovery facilities and command centers? It's funny, but I actually got to see "The Big Board" of Hollywood and Dr. Strangelove fame. I even sat in the general's chair. Today, I see these "war rooms" turning up in lots of commercial enterprises. No, I don't see Slim Pickens or George C. Scott in them, but they are there, and they are now called *Recovery Operations Centers (ROCs) or Recovery Management Centers* or other names. They are what they are, however, and that is command and control, which is in itself a military term.
- In decades past, who else but the military meticulously documented elaborate restoration plans — down to the level of exactly what alternate routes were to be established, depending on which major hub was lost. We had to do a lot of this with manual patch panels, but today essentially the same function is being performed with digital cross-connect systems (DCS) and self-healing networks.

Plainly, today not only the military but also many commercial organizations demand a Johnson Space Center level of command and control. Time frames for recovery are shorter than ever. Dependence on telecommunications and networks is higher than ever. The threats faced by organizations, even here in the United States, are more diverse than ever, to the point where commercial organizations can actually be the equivalent of military targets. Consider these sobering realities:

Telecommunications hubs are no longer targets for the Russians, but they do present tempting targets for terrorists. If somebody has to attack a major bank, defense contractor, energy company, or other target, they don't have to target that organization's facility for they can target its central office. For years we spoke about the impact of a bomb at 30 Broad Street in New York, or at 4100 Bryan Street in Dallas. That exposure has not gone away and, in fact, in many ways it has gotten worse, as we will discuss in later chapters.

With the advent of so many call center operations moving to India, or manufacturing organizations moving to China (the list goes on), today's commercial organizations do indeed demand for 10 minutes clearance time on international circuit failures. There is no reason to believe that these recovery time frames will become anything but shorter in the years to come.

Furthermore, we have not yet even spoken about dependence on the Internet. Now let's get this straight. In many companies, the most mission-critical applications traverse a network that nobody owns. How's that for reality? So, why do so many companies climb aboard? Well, the first thing to consider is the nature of the Internet that, in and of itself, is "warmed-over 30-year-old military technology." The Internet, with regard to backup and recovery, is a proverbial two-edged sword.

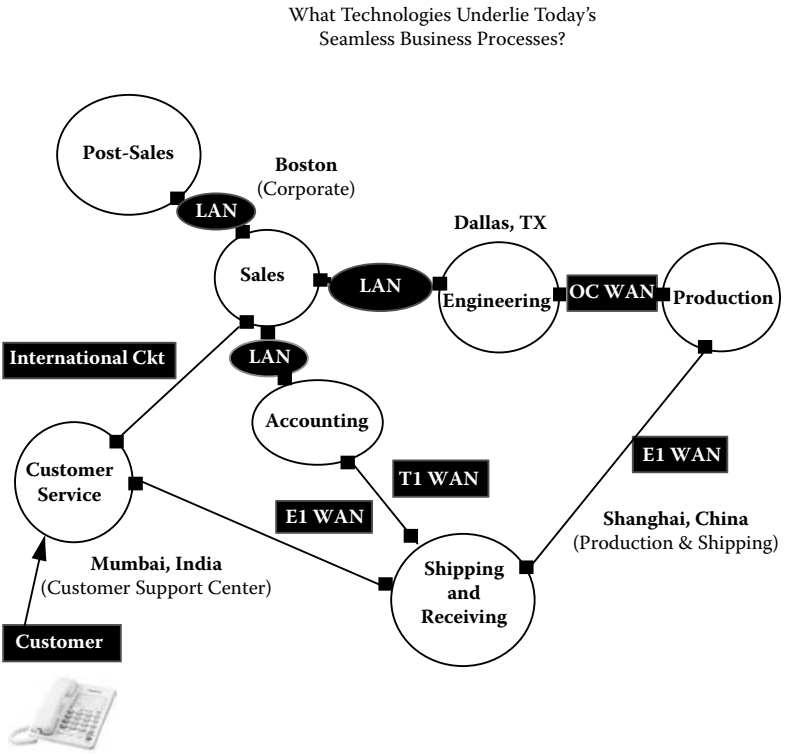


Figure 4.2 The 100,000-foot technical view of a hypothetical seamless company.

On the one hand, it is easy to make a Dallas (VoIP) telephone number like mine, (214) 888-1300, work in India almost instantly, or vice versa. All you need is a good access to the Internet and the change is transparent to the caller. On the other hand, come all the concerns of standards for network vulnerability to every manner of hacker, virus, and threat that nobody owns. What makes the Internet work so well is that it has been characterized as "distributed intelligence with nobody in charge" (kind of like my office). That means every node is a little bit smart — just enough to get messages through in a hypothetical 1970 scenario that placed the AT&T toll offices in the upper atmosphere after a Russian strike. The same characteristics of the Internet that helped the military planners of yesteryear help the contingency planners of today.

So, if all of these past practices were so good, even with the relative junk we had for technology in the 1970s, just imagine what can be done with the same fundamentals, but employing today's technology. The documentation, coordination, and CCC (command, control, and communication) issues, as I have already stated, have changed surprisingly little. What we could not do in the 1970s were overlay things like wireless phones, nationwide walkie-talkies, text pagers, laptop computers, and

other tools that simply did not exist then. Therefore, if you know what to borrow from the past and can combine it effectively with today's technology, you can implement a most resilient plan for far less money in a surprisingly short time.

So, what can you borrow from past plans? The list is limitless but includes items like the following:

1. Who owns the building? It would be a good idea to find out before you start, if for any other reason than to find out who "stays" and who "goes." After a major disaster, some of your workforce will have to establish processing at another location whereas others presumably will have to stay and clean up.
2. How do people get cash? One thing companies often overlook is how to get cash to employees who must travel to a "hot site." In a Katrina-style disaster for example, ATMs may not work; banks may be closed. I have seen examples of companies that work with their banks to dispense cash (and account for it, which is another chore) upon declaration of a disaster. This is often accomplished at prearranged branches or even from specially equipped vans.
3. Are you a union shop? If so, you will need to have representatives of organized labor involved.
4. What about office supplies? Think you will need pens, pencils, paper, and a place to sit? Better plan on some procurement people in the loop with PO's (purchase orders) presigned and "in the pipe" so that you can bring in essential supplies quickly.
5. When was the last time you had your hair done? Are you ready to look good on TV? If not, better think about a media relations person. This is a lot more important than you might think. The news chopper will be on the scene minutes after a disaster. As your people come out, the media representatives will be talking to them. You know how these things work. The first three will have the good sense to respond, "We have the situation under control." The fourth one, however, will inevitably say something like "they are all *dead* in there … we'll never open again!" Now, which one do you think will be on the 11 P.M. news?
6. Are you ready to search the home of a seriously injured or dead employee, with their family members there, for backup tapes you need to restore your data center? If not, better plan on some formal off-site storage today and a media retrieval person to go after it when a disaster is declared. I don't mention this last item to be morbid, but just imagine being placed in such a position. "Sorry about Karen's untimely death, Bruce, but we really need to find those tapes."

In summary, many of the same procedures we have employed in military — and mainframe — systems for years can and should be adapted to today's environment and be leveraged by today's technology. You should draw on some of the good commonsense fundamentals of a workable contingency plan, which change relatively little over time. I'm aware that as a technologist you know how to leverage

today's technology as you plan. While you are at it, why not dust off some of those old mainframe recovery plans? Equipment like PBXs and routers are beginning to look and act like yesterday's mainframes and now demand comparable levels of protection because they are just as important today.

CHAPTER 4
WORKSHEETS

WORKSHEET No. 1

Identifying the Resources You Will Need

The following personnel have prior military experience that encompasses contingency planning:

Name	*Department*	*Branch*	*Remarks*

Additional Comments

_____

_____

_____

_____

WORKSHEET No. 2

The following personnel have commercial or "Big 4" experience that encompasses contingency planning:

Name	*Department*	*Remarks*

Additional Comments

_____

_____

_____

_____

WORKSHEET No. 3

List your "top ten" indispensable "command and control" numbers that must be in service immediately after a disaster.

Number	*Function*	*Remarks*

Additional Comments

_____

_____

_____

WORKSHEET No. 4

Taking the same "top ten" command and control numbers from the previous worksheet, state where they must ring after a disaster, and within how many minutes.

Number	*To Where*	*How Long?*	*Remarks*

Additional Comments

_____

_____

_____

_____

WORKSHEET No. 5

Location of Backup Site

The company's backup location for executive management team (EMT) functions is:

_____
Name

_____
Address

_____
Suite

_____
City, State, Zip Code

_____
Phone

_____
Fax

_____
E-mail

Remarks:

_____

_____

_____

_____

_____

_____

WORKSHEET No. 6

The following equipment/technology is required at the backup site, either in advance or within two hours of a disaster declaration. Check the ones that apply to your company and make additional entries as needed.

Item	*Quantity*	*Responsible Department*	*Remarks*
Telephone			
E-mail			
Wireless LAN			
Laptops			
Fax machines			
Attendant positions			
IADs (VoIP)			
PCs			
MACS			
Displays			

WORKSHEET No. 7

The following equipment/technology is required at the damaged site within two hours of a disaster declaration. Check the ones that apply to your company and make additional entries as needed.

	Item	*Quantity*	*Responsible Department*	*Remarks*
	Security personnel			
	Medical personnel			
	Hard hats			
	Identifying vests/ IDs			
	Flashlights			
	Wireless phones			
	Blackberry			
	PDAs			
	Copies of Recovery Plan			

WORKSHEET No. 8

The following equipment/technology is required at the Recovery Center (as differentiated from the EMT location) within __ hours of a disaster declaration. Check the ones that apply to your company and make additional entries as needed.

	Item	*Quantity*	*Responsible Department*	*Remarks*

WORKSHEET No. 9

Sample:

"Hot Lines"

Think of all the other ways you can maintain command and control using today's technology.

Check If Available	*Item*	*Remarks*
	Conference bridge	The number is:
	Low-power AM radio station (for Employee and Emergency Instructions)	Dial ____ kHz on your AM radio dial
	Two-way radio or Nextel phones	Can be picked up on site at _____ From _____

WORKSHEET No. 10

Extraordinary Command and Control Procedures for Loss of Major Telecom Hub (see Chapter 1 for details)

Make sure personnel are briefed on what to do if the following conditions occur. Make additional entries to your individual plan as needed:

- *No or Slow Dial Tone*
  - Instruction: Blow or speak into the mouthpiece. If dead, try another phone. If not, wait 60 seconds. In widespread disasters, dial tone is slow but may still work.

- *Fast Busy When Making Calls*
  - Keep trying; it may take hours because the network will be congested. Try other mediums such as VoIP or wireless.

- *All Circuits Busy Recording*
  - Keep trying; it may take hours because the network will be congested. Try other mediums such as VoIP or wireless.

- *Others*

_____

WORKSHEET No. 11

Extraordinary Command and Control Procedures for Loss of Major Telecom Hub (see Chapter 1 for details)

1. Responsible person/department for the building	(Area code and number)

2. Responsible person/department for security	(Area code and number)

3. Responsible person/department for cash disbursement to employees	(Area code and number)

4. Responsible person/dept. for union liaisons	(Area code and number)

5. Responsible person/dept. for office supplies	(Area code and number)

6. Responsible person/dept. for public relations and media affairs _____ (Area code and number) _____

_____ _____

_____ _____

_____ _____

7. Responsible person/dept. for grief counseling _____ (Area code and number) _____

_____ _____

_____ _____

_____ _____

8. Responsible person/dept. for _____ (Area code and number) _____

_____ _____

_____ _____

_____ _____

Chapter 5

Developing Operating and Security Standards

Leo A. Wrobel

Contents

Standards for Buildings, Networks, and Other Infrastructure 99
Physical Standards — Small Installations 101
Physical Standards — Large Installations 102
General Housekeeping 103
Building Entrance Facilities 110
Chapter 5 Worksheets 129

Standards for Buildings, Networks, and Other Infrastructure

It was once said that there is only one kind of disaster, the messy kind. If any of you has ever had water, for example, in a place in your building where it did not belong, that's pretty messy. One example that comes immediately to mind for me is a client we had whose cable risers had metal mesh floors (that opened from one floor up and down to adjoining floors) and which also contained water pipes. To add to this issue, the cable risers were also adjacent to the restrooms. We cited this issue in an audit, not so much because of the pipes, but because if one of the restroom toilets backed up, the water only really had one place to go: straight down the riser. (Sharon and I have seven children. Every child backs up a toilet at least three times in its life. Therefore, with firsthand experience of 21 such episodes, we had a high degree of sensitivity to this issue.) All kidding aside, we determined that water could be a problem for this client.

About three months after our report, we received a call one Monday morning that the client had sustained a significant disaster. To be completely honest, my first reaction was that we caught it in our report. As it turned out, it was water in the cable risers but not from the toilets. Apparently, one of the pipes in the riser had sprung a leak early the day before, on Sunday. The water fell four stories to the bottom of the riser in the subbasement to the only place in the whole organization it could not go: the main uninterruptible power system (UPS). It was told to me that the flash could be seen from the subbasement all the way to the third floor. What it meant was that all primary and backup power instantly went "poof." Imagine the impact of a hard shutdown on all of our mainframe, open, and telecommunications systems at this moment. Now, multiply it by about ten because this particular client was huge. Much to their credit, business was restored by the end of Monday. Monday, as it turned out, was also a holiday. The Tuesday after a holiday, however, is usually one of the busiest days they have for any call center. If they had not recovered by then, the disaster would have been much worse.

There are a few lessons to be learned from this example. One is about water. Another is about UPSs and the false sense of security one can have by thinking UPS systems do not fail. They do. Yet another lesson can be learned from how this company reacted to ensure that a disaster of this type never happened again. Their solution was amusing, but thoughtful.

Immediately after the disaster, the company brought the staff together and isolated the water pipes in the cable risers. All types of solutions were proposed. The meetings in fact lasted several days. At one point, engineers were even proposing special coatings for electrical fixtures that had to be in the risers. It was expensive, unusual, and nobody really had any experience on what the long-term impact of coating everything might be. In the middle of one such meeting, one participant popped up with a remark. "Why don't we just install outside electrical fixtures?" With that, the collective, self-inflicted slap to the foreheads of every engineer in the room could be heard about 5 mi away. Outside fixtures for electrical items are available cheaply, and can be found in any Home Depot. What would have been a very expensive project had a cheap, ubiquitous, and readily available solution immediately at hand. In the heat of the moment, however, nobody thought of it. You will experience many moments such as this one as you produce your recovery plan. For this reason, it is also important to involve as many others as is reasonably possible, as any member of the team may see the solution to a problem that everyone else is missing.

With this in mind, what kinds of issues could be simmering in your building, seemingly under your nose, waiting to hit you some rainy Sunday afternoon? Some of the more common ones are shown in the following text.

Physical Standards — Small Installations

Physical standards for small installations are items related to routine housekeeping, or commonsense-type items, which should apply to any good equipment installation. An example is access to equipment rooms.

We have heard many stories in the past about how allowing unauthorized users into equipment rooms has wreaked havoc with users of technical systems. One story that we've heard involves a drywall contractor doing a job for a company on a weekend. After completing the drywall job, the contractor in question used the connecting blocks on telecommunications equipment, located in the janitor's closet, to clean the drywall mud off their trowels. The result was an extended outage the following morning when the drywall contractor was long gone.

How many small telecommunications installations does your company have inside or co-located within the janitor's closet? Surprisingly, this is very prevalent within companies, and a cause for concern when unauthorized or uneducated people have access to technical equipment. As a rule, when feasible, equipment should be installed in a location other than a janitor's or custodial closet and be secured and locked to prevent access to anyone other than authorized persons.

A second issue to consider in basic physical standards is housekeeping. A no-smoking policy, for example, should be strongly encouraged within the equipment room.

Encouragement of other items should include fire extinguishers of the appropriate type and posting of instructions for its use. Reasonable precautions should be taken to ensure that the temperature of the room conforms to the manufacturer's specifications and that the room does not get unduly hot or cold. Also, power to the unit within the equipment room should conform to the manufacturer's specifications in terms of spikes, sags, brownouts, blackouts, and type of power. The general condition of the room should also be evaluated, in terms of whether the room is too damp or too dusty.

It's generally relatively easy to devise a set of standards for non-mission-critical telecommunications equipment in small installations. Your standard should say something similar to this: "The company bought this equipment, the shareholders paid for this equipment, and it's our responsibility not to let the equipment be stolen, broken, wet, or otherwise damaged." Other than this, except for the possible exception of a maintenance contract, very little need be done to protect non-mission-critical small installations for telecommunications.

Servers and Telecommunications in Janitors' Closets Are an Open Invitation to Trouble

LOOKING INSIDE RISK POINTS IN YOUR BUILDING

- Entrance facilities (cable and people)
- Manhole serving your building
- Riser cables, fire stopping
- Shared closets and cable spaces
- Distribution or overhead feeder cables
- Building security/parcel pass system?
- General cable condition
- Use of conduit
- Grounding
- Contact with electrical cables
- Power and generators
- Pipes and shut-off valves

Physical Standards — Large Installations

Mission-critical small installations and large telecommunications installations of all types present an entirely different type of problem and should be much more intensively protected. The remainder of this section will deal with physical and environmental standards for large and for mission-critical telecommunications installations.

Access to Equipment Areas

The Telecommunications Standards Document should bar any unauthorized individual from equipment rooms unless they have a documented reason to be there. This includes other employees and visitors of all types. The room should employ additional protection, such as locks on the door, cipher locks, and other improvements. As with the computer center, any large glass areas in the building should be considered for either reinforced glass or masonry to prevent damage from outside sources or intrusion.

General Housekeeping

In terms of housekeeping in the large network installation, a number of items should be mandated. This includes a ban on eating, drinking, smoking, or open flames of any type within the large network location.

Evaluation of Power

Power to and the environment of these large network locations must be thoroughly tested. In areas where mission-critical applications are supported by large telecommunications systems, the use of such precautions as uninterruptible power supplies should be seriously considered.

Fire Protection

Other systems, such as fire extinguishers, fire alarms, and Halon, etc., should be on a par or equivalent to those installed at large computer centers, which provide similar functionality in terms of mission criticality. They include smoke and particle detectors, fire-escape plans, moisture detectors, dry-pipe sprinklers, Halon systems, and other miscellaneous items. These may also include such steps as labeling water pipes for fast shutoff in the event there is a leak in the equipment room. Other items that we have typically seen in such plans include sheets of plastic or equipment covers, which can be thrown over equipment quickly in the event of any type of water problem in the building.

An outfit called CoverGard specializes in providing fitted plastic covers for equipment for use in just such situations. Because they are conveniently located in pouches on the side of the equipment, they can be quickly pulled out and deployed in the event of any type of water problem.

Change Control for Mission-Critical Equipment

Any mission-critical telecommunications hub should employ network and change control management. These should include a listing of persons authorized to make major software changes. They should also include procedures for the password protection of maintenance functions, particularly those accessed from off-site locations. Also, procedures should be in place that mandate a full backup prior to any major software changes, to allow for fallback in the event something goes wrong. See Figure 5.1 and Figure 5.2.

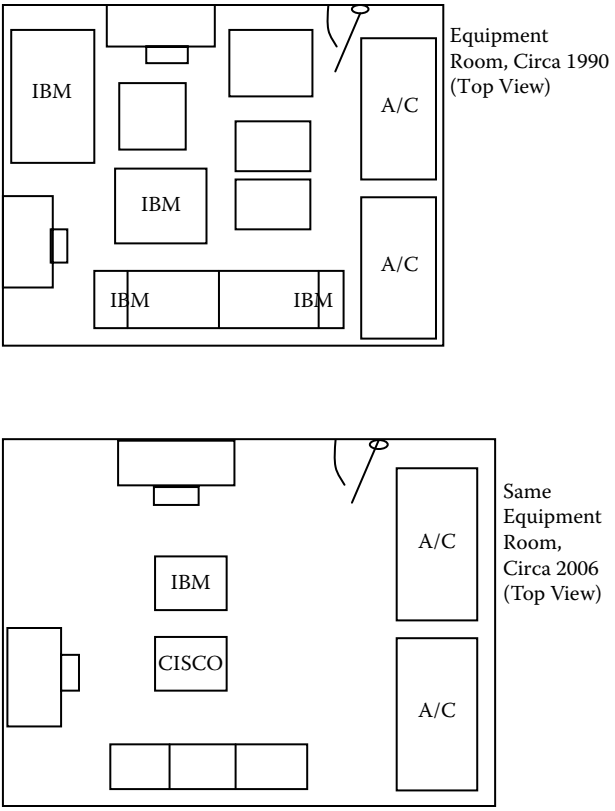


Figure 5.1 Is this your situation? Equipment room (circa 1990, 2006).

Disposal of Confidential Materials

Other items may also be included in this section, such as, "How to Dispose of Confidential Materials." It is imperative that any article that contains an access code or other confidential information be shredded, just as in the computer room, to avoid it being intercepted by "dumpster divers," who delight in going through corporate trash and selling items of value to the highest bidder.

Standard Policy on Communications Privacy

Your company may also want to consider retaining a law firm or consultancy to draft a policy on privacy for telecommunications. Over the last few years, privacy issues have emerged as an upcoming problem to the telecommunications manager. For example, in one company, an employee ran an illegal bookmaking facility from a voice mail system, and did so for several months. The company, after monitoring activity in the voice mail system, decided to investigate, and discovered what

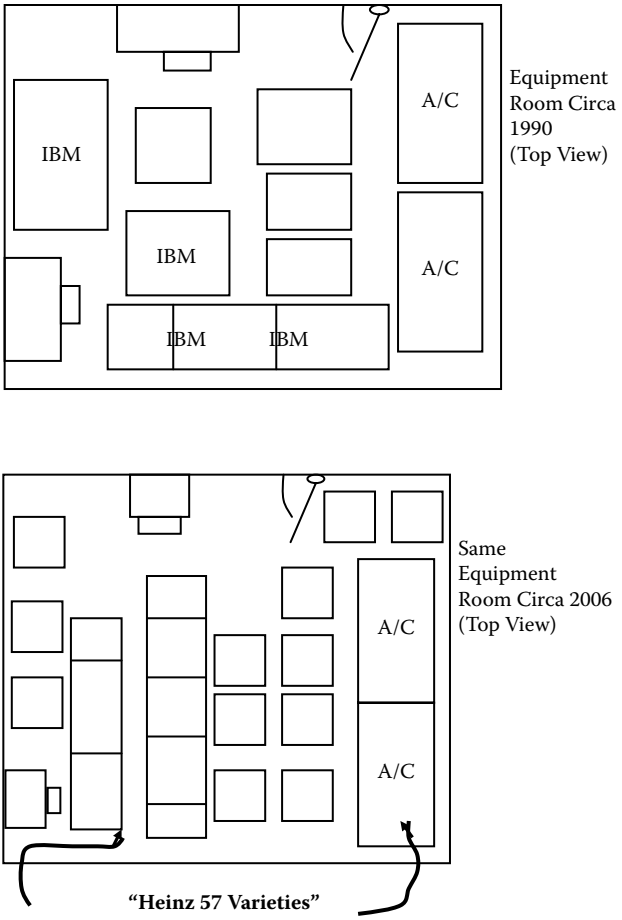


Figure 5.2 Or is this your situation? Equipment room (circa 1990, 2006).

was going on. Afterward, they fired the employee for running the illegal gambling operation from a company-owned voice mail system. The employee, in turn, sued, stating that the company had no right to monitor private conversations, and was subsequently reinstated.

Policies on privacy within corporations run the entire spectrum. At one end of the spectrum, the corporation may say, "We own the voice mail system and will listen to any conversation anytime we want." On the other end, the company may say, "Regardless of the fact that we own the voice mail system, you, as an employee, may be assured of absolute privacy at all times." Both of these stances can be points of debate; however, it's important that the company's policy be documented, regardless of what it is, in case a similar situation to the bookmaking operation described earlier occurs.

Even though the final word on telecommunications privacy has not yet been written, by having a policy on privacy documented, your company will be much better situated should litigation arise from unauthorized use of telecommunications resources or other occurrences.

Lastly, users should be advised that telecommunications is not a secure media, and privacy of conversations may, from time to time, be compromised. Cellular telephones are a good case in point: anyone with a $200 bear scanner can monitor cellular telephone calls. The telecommunications department may provide information on encryption devices for facsimile transmissions, cellular telephones, and other items. Users should be aware, however, that in most cases, telecommunications facilities are not a secure media, and even in organizations where privacy is guaranteed, circuits may from time to time be subject to maintenance monitoring, which could compromise sensitive conversations.

Other Items for Inclusion in the Standards Document

Now let's look at a few items related to disaster backup and recovery, which should be embodied in the Standards Document. Let's say, for example, a telecommunications manager is looking to back up critical "800" numbers. Which 800 numbers are most critical? What is the policy on providing priority and restoration for 800 numbers? How does an end user in a different department (from the telecommunications manager) request priority or emergency backup of 800 numbers? These should all be defined in the Voice Network portion of the Telecommunications Network Recovery Plan — not only 800 numbers, but all types of incoming and outgoing numbers.

Other items, such as how frequently this listing should be updated, should be defined in the Standards Document. Similarly, on the data network side, all critical private line circuits, whether they be router links or other types of dedicated circuits, should be defined in terms of mission-criticality and time frames established for how quickly they must be recovered.

Network diagrams should also be referenced on where they can be found in a disaster, as well as what the complement of circuits to a recovery center may be, if one is used.

All types of callout and escalation lists will also be defined in the Standards Document. For example, where is the correct repository to find accurate and up-to-date home telephone numbers of employees? This varies from organization to organization. Sometimes, Human Resources is the best source. Sometimes, it's the company telephone directory. Sometimes, it's none of the above.

The methodology that will be used to take these critical telephone numbers and transport them to the recovery plan must also be defined. Optimally, this is done through a process called "importing." In a distributive LAN/open environment, these items can sometimes be imported from Human Resources or from other departments by object-linking files. In other environments, it becomes the responsibility of a person or department to actually walk over to the department that

possesses the list, make a copy, bring it back to the telecommunications department, and import it into the plan in that fashion.

Suffice it to say, at this point, that all critical vendor, carrier, and employee call-out and escalation lists must be imported from known good sources, and these sources must be identified in the Standards Document.

Open Systems Security Standards

A few other items that may be identified in the Standards Document include Interconnection Standards for LANS. For example, let's say a LAN user in the Finance Department takes great pains in ensuring that the LAN is operated to a high standard of integrity. This might include regularly running programs to detect viruses, for example. Because a LAN in the Finance Department would probably be considered mission critical, this user probably conforms to a very high standard of operation for his or her LAN.

Now, let's take another case of a LAN being operated, perhaps in a sales branch. The LAN manager of this particular system is running a hack outfit. His people are downloading public domain software from bulletin boards, readily transporting floppy disks, and putting the LAN in the Sales Department in distinct danger of being contaminated by outside computer viruses. This LAN in turn utilizes a telecommunications link to connect with the LAN in the Finance Department. In such a situation, the manager of the Sales LAN refuses to comply with accepted standards for the operation of his LAN and, as a result of this, puts a mission-critical LAN in danger of being contaminated or otherwise inoperative. It may in fact become the responsibility of the telecom manager to pull the plug before this happens. Hence, the telecom manager becomes the policeman to prevent virus contamination of multiple distributed LANs that use their network to connect. Issues such as this one should also be defined and agreed upon in the Standards Document.

Lastly, any command-and-control features that the Corporate Telecommunications Department provides should be defined within the Standards Document. These may include numbers for conference call bridges to call in people after a disaster; they may include numbers for "800" services where employees can dial to get up-to-the-minute information on the status of a disaster and other issues relevant to command and control.

The Standards Document's Place in the Recovery Plan

A Telecommunications Standards Document could be designed to be an integral part of the Telecommunications Recovery Plan. This is often done. Our individual preference, however, is to provide the Standards Document as a completely separate stand-alone document from the Telecommunications Disaster Recovery Plan. This

is done essentially for two reasons. One, the Disaster Recovery Plan should be as lean a document as possible to provide for easy understandability in the event of a disaster. This is difficult to do if it's cluttered with numerous telecommunications standards. Second, the Standards Document is not intended to be an emergency document, but to be a document that dictates the day-to-day conduct of business within the telecommunications environment. As such, we would expect the Telecommunications Department to consider this document to be a living, breathing document that governs the day-to-day conduct of the Telecommunications Department, not an emergency plan to be pulled out only when required. This document would be referred to regularly and be interdepartmental in scope. The Standards Document will become the conceptual foundation for the Recovery Plan. In the later section, when we write the Disaster Recovery Plan for Telecommunications, we will often refer back to the Standards Document when dealing with Emergency Response Procedures.

The Standards Document for Telecommunications should be written only with the support and participation of other related departments. Your company, for example, may want to consider formation of a Telecommunications Standards Committee of perhaps a dozen members to decide very broad company-based issues such as which vendors, software, and equipment the telecommunications department will support for the end user. In the absence of this type of control, namely, a listing of supported services and vendors, it becomes all too easy for end users to subscribe to every type of service and equipment available and to spread the telecommunications department very thin as far as knowledge level and support services are concerned.

The Telecommunications Department can only be expected to know so many software and hardware systems and still provide effective support. Similarly, this causes a severe drain on resources in a disaster when the Telecommunications Department must scramble to restore innumerable systems and software packages at a recovery center or alternate location.

By the same token, the end user needs some flexibility in these areas to be productive and make the company the most money. Therefore, we also don't want to be too rigid in our standards of supported software and services.

The Telecommunications Network Standards Committee allows a forum for users to introduce new technologies and for them to be evaluated by qualified technical people in terms of cost, in terms of benefits, and in terms of organizational drain on resources.

Telecommunications-Specific Security Practices

For many years, large mainframe computer centers have employed operating and security standards to ensure continuity of the recovery process in a disaster. The

telecommunications installation is no exception. This is especially true today, when large telecommunications nodes look and act more like computer centers all the time. Therefore, we need to look at our operating and security practices such as changing passwords on equipment, protecting in-dial equipment, and a host of other aspects of the planning process that may or may not be common knowledge to a telecommunications professional.

In the following sections, we will discuss remote access and how to safeguard the environment when people are installing "Go To My PC" and other software improperly or without authorization. We'll also discuss access to maintenance ports for items such as voice mail and digital cross-connect systems and multiplex systems. Most of the upcoming materials, however, will look at physical security standards, including what constitutes a good installation, to protect against disasters before they happen. The planner will want to concentrate efforts on three major areas:

1. Looking inside: The following section will concentrate on specific areas to address within the building. These will be familiar to persons who have engaged in "classical" computer recovery operations for mainframes or other systems housed within the building.
2. Looking at the local telephone loop.
3. Looking at the long-distance interexchange carrier: Don't forget to evaluate telephone company vendors using both the criteria outlined in the coming chapter as well as the audit procedures for telephone companies outlined earlier in this text.

Looking Inside

During this initial effort, the recovery planner will be interested in everything that could cause a disaster *within the building.* These include possibilities such as fire, water intrusion, and various physical security items. This first phase will be very familiar to people who are already well versed in mainframe recovery planning because the same kinds of security and installation standards that apply to large computer room installations generally apply to large telecommunications installations. Some items that deserve a critical look include the following.

Physical Security

Remember, as we stated earlier in the book, there are a number of people within the organization who think they own the building. MIS Managers, because they "own" the computer room, feel that they are the rightful owners of the building. There are also persons at the front desk with blue suits and badges who think they own the building.

Physical security is very important for a number of reasons. Unauthorized persons in the building, for example, could wreak havoc on technical equipment by shutting something down unintentionally.

Theft of Equipment

As systems become more and more distributed, DOS-based LAN systems are becoming common in today's decentralized environments. Unlike the IBM systems of the past, these systems tend to "get legs" and are commonly stolen. Therefore, part of the physical security process should include a parcel pass system (see Parcel Pass form below) which ensures that the person leaving your building with a laptop computer or other equipment really is entitled to leave with that equipment. This includes not only laptops, but other types of equipment as well. The successful parcel pass system should include a mechanism whereby a user coming into your facility signs in and declares his notebook computer, modem, or whatever he happens to be carrying with him. It should also include an inspection of briefcases or any carry cases large enough to hide small equipment that could be used to get it out of the building.

Building Entrance Facilities

The physical audit of your facility should include all cable entrance points into and out of the building. For example, many companies pay large sums of money to telephone companies for diverse cable access. It makes little sense, however, to pay a lot of money for diverse cable access only to bring this cable through the *same building penetration* into your facility. Any common location at which the cable comes in is an obvious point of failure because of people working in the building, fires, or any number of causes. Therefore, it is a pretty good idea to look at where these facilities come in and assess them for single points of failure. Similarly, for cable that goes between floors, there are a number of areas to look at here, as well. All facilities between floors should be fire-stopped with a fireproof material to keep a fire in an equipment closet below your floor from spreading to yours. All of these facilities should be locked and secured from unauthorized personnel.

PARCEL PASS FORM

This form must be completed to bring any equipment into the building.

NAME _____

COMPANY _____

TELEPHONE _____

Equipment Description _____

_____

_____

Purpose _____

_____

_____

(Above space to be filled out by person bringing in equipment.)

NAME _____

TITLE _____

PHONE _____

DATE _____ TIME _____

SIGNATURE OR INITIALS _____

(Above space to be completed by employee signing in equipment.)

Fire-Retardant Cable

Fire-retardant telecommunications cable should be specified when possible. Traditionally, this has been Teflon cable; however, other materials are beginning to be used for fireproof cable as well. These include HALAR and Kevlar (yes, the same material used in bullet-proof vests). The preponderance of the cable within your facility, however, is probably PVC (polyvinyl chloride), which does burn and create nauseous fumes as well as hydrochloric and sulfuric acid compounds when wet, such as from a fireman's hose. It is also a good idea to have a fire extinguisher in all cable closets and instructions prominently posted so that people are well versed with its use. A no-smoking policy is an absolute necessity in a cable vault because cable can produce hydrogen gas, which is very explosive when mixed with oxygen (remember the Hindenberg disaster?).

Fire Suppression Systems

Today, there are primarily three means of fire suppression within large commercial buildings. These are the following:

1. Carbon dioxide
2. Halon
3. Sprinkler systems

We will discuss these systems briefly, concentrating on the inherent strengths, weaknesses, and risks associated with each.

Carbon Dioxide

Carbon dioxide is very effective in fighting fires because it interrupts the combustion cycle by removing the oxygen from the air. However, there are two problems with carbon dioxide. First and foremost, it has a tendency to *kill* people in the room when it goes off. Obviously, if carbon dioxide removes the oxygen from the air, people and other living things cannot be in the room with it. Therefore, carbon dioxide is primarily used in uninhabited areas. Next, there is a second problem with carbon dioxide, namely, thermal shock. Any Vietnam era veteran, for example, knows that the quickest way to cool down a six-pack of beer is to put it in a garbage can, get a CO2 fire extinguisher, and give it a good long blast. The beer ends up nice and cold because the fire extinguisher's contents come out at 150°F below zero. Although that is a funny and amusing story, it does graphically illustrate a point, that is, if people don't asphyxiate in an environment with carbon dioxide, they will probably go into thermal shock because it is very cold. This is another reason why carbon dioxide is not used in areas where there are people.

Water-Based Protective Systems

Sprinkler systems are very effective at fire suppression, and more and more commercial buildings are demanding that sprinkler systems be installed, whether or not equipment is being installed in the location.

There are generally two schools of thought with regard to sprinkler systems. The first is, "Thou shalt never have water over electronic equipment." The second school of thought is, "Go ahead and install sprinkler systems over the equipment." In fact, you may even allow your equipment to get wet and it can still be restored. Let's consider the second. Today, business interruption insurance providers, fire departments, etc., insist on the installation of sprinklers even within an equipment room. The reasoning is that if the fire alarm goes off, the power to the equipment is cut anyway and the sprinklers go off too, saving the building. The equipment then is obviously wet, but (they say) it can be restored.

In these situations, engineers for the equipment come in, literally pull the boards out of the equipment, dip them in special solutions, and use a blow-dryer to dry out the inner guts of the equipment. Afterward the equipment is reassembled, tested, fired up, and everything is just perfect. Correct? Actually, there are advantages and disadvantages to this approach. The advantage, obviously, is that it is much cheaper to repair equipment that has become wet than to replace it. Some general industry estimates say that replacing selected components of major systems is still up to 60 to 70 percent cheaper than to replace it altogether. And there are companies that specialize in this type of work. The disadvantage is that equipment that is restored in this fashion can be trouble-prone in the future.

Let me explain. For the next several months after the disaster, whenever intermittent troubles pop up, and they will, the user can never be sure of the cause. One possible cause may be that the equipment could have been hot when the water hit it. By hot we mean both electrically hot and physically hot.

If the equipment was electrically hot, the short-circuiting of components could have caused problems within the individual components themselves.

In the case where equipment is physically hot, a sudden dash of cold water, causing rapid contraction of circuit boards, could also have caused problems, particularly in today's multilayered printed circuit boards.

Lastly, consider the effects of static charge on circuit boards. Most of these boards were designed to be installed while wearing a wrist strap, taking much care to abide by static guard procedures. What do you suppose the effect is on these boards when someone literally takes a blow dryer, which generates all kinds of electromagnetic interference, and runs this inside your equipment to dry it? Again, we have to consider this as a possible cause of intermittent trouble later on. Additionally, consider the condition of the water within your sprinkler systems. It is a fairly well-known fact that distilled water is an insulator. However, the water in your sprinkler system is far from pure and distilled water. In fact, many times when a sprinkler system goes off, the water initially runs black from the pipe until the pipe cleans itself with water coming in. Because this water obviously has all types of oxidation and iron in it, it is a very good conductor and can really play havoc on your equipment, particularly when the equipment gets wet while it's still electrically hot.

Generally speaking, sprinklers don't leak. This may be surprising, but sprinklers are pressure tested, and they are installed according to very exacting specifications. The problem is that people cause most disasters, and disasters involving sprinklers are no exception.

In equipment rooms where there is a ten-foot clearance for sprinklers, it is almost guaranteed that someone will try to roll an 11-foot crate through, and perhaps break off a sprinkler head, causing a problem. We have also seen instances of people crawling through a suspended ceiling area, perhaps to pull cable, and stepping on a sprinkler pipe, causing a leak and a mishap in that fashion.

One way of avoiding these types of problems is to use some type of a dry pipe, pre-action, or pre-charged sprinkler system. We will talk for a moment about each type.

Dry Pipe Sprinkler System

A dry pipe sprinkler system does not actually have the water overhead in the equipment room. Instead, it is filled with either pressurized air or nitrogen. Typically, this system is used where freezing is a possibility. The dry pipe, as the name implies, keeps the water out of the equipment room until such time as the fire alarm is

tripped. An electromechanical device and a dry pipe valve, held by air in a closed position and located in a heated space outside of the equipment room, keep the water safely outside the room until such time as it may be needed. When the first alarm system trips, the valve opens, allowing the water into the pipe and inside the equipment room. Then, when the filament for the sprinkler system actually melts, the water will come out at that time. Be aware that even in a false alarm, the valve will open, and the water will enter the pipe in the equipment room. After a false alarm of this kind, it is usually necessary to call the contractor who installed the sprinkler system to evacuate the water from the pipe to maintain the value of the dry pipe system.

Pre-Action and Pre-Charged Sprinkler Systems

Pre-action and pre-charged sprinkler systems work on a similar basis, some using an inner gas inside the sprinkler system to hold the water back and others using a valve. Two events must occur before the system discharges: (1) The detection system must recognize a fire and then open the pre-action valve, which will essentially create a wet pipe sprinkler system that will allow water to flow into the system's piping; and (2) a releasing of separate sprinkler heads needs to occur before water flows onto the fire. For more information on these types of sprinkler systems, contact your company's authorized fire prevention company.

There are alternatives available if your equipment does get wet. First, the equipment can be professionally restored back to operating condition by a company that is specialized in these types of emergency restorations, such as BMS Catastrophe in Fort Worth, Texas. This is a very cost-effective way of accomplishing the equipment replacement and recovery process because there are several competent companies that specialize in these services. However, in mission-critical equipment, be very careful. When in any doubt, replace the component because intermittent problems will plague the equipment, perhaps for months after the disaster takes place. We will have more information about these companies later in this text.

Use of Halon Systems

Another option for fire suppression is a Halon system. Halon works in somewhat the same fashion as carbon dioxide with one major exception. Halon can be used in rooms with humans, and is not harmful to breathe or be exposed to. Rather than taking the oxygen out of the air or displacing the oxygen as carbon dioxide does, the Halon molecule interrupts the combustion cycle required to sustain a fire. To have a fire, you must have three things: heat, combustible material, and oxygen. Rather than depleting the oxygen, Halon interrupts the combustion cycle and puts out the fire. In actuality, it only takes a small percentage of the oxygen out of the

air; therefore, it is possible for people to remain in the room and breathe during a Halon discharge.

First, Halon depends on a closed, confined area to be effective. For example, if the door to your computer room is open at the time the Halon discharges and if this door opens outward, the force of the discharge may just be enough to open that door, blow the Halon out, and allow oxygen into the room. This, in effect, would compromise your system and allow the fire to burn. Also, often the integrity of the room itself is compromised by people putting holes through sheet metal walls to run cable, water pipes, or similar items. This is especially a concern above ceilings and below raised floors. Someone will knock a hole under the raised floor, for example, to run cable, and if Halon discharges under the floor, again, the integrity of the Halon is compromised by the hole.

While we're on the subject of discussing Halon dumps under the floors, here is another key consideration: Halon is not effective against very deep-rooted electrical fires, which require very little oxygen to burn.

There are other issues associated with Halon, such as environmental issues, which will influence the decision on whether to use this fire prevention method. Halon itself is a CFC (chlorofluorocarbon), similar to the refrigerants used in refrigerators and automotive air-conditioning systems. As such, it damages the ozone layer of the atmosphere. The government in the United States and, indeed, many countries are beginning to phase Halon out. Although a complete ban on Halon does not appear to be on the cards, it is going to become prohibitively expensive to use, both owing to the government taxing it and its limited availability and production. Already, there are laws in place that mandate systems should recover Halon and other types of CFCs and not vent them into the atmosphere. In short, if you have Halon in place, and you do have a Halon discharge, it will be very, very expensive to replace the Halon after the event.

Other Fire Prevention Concerns

While we are thinking in terms of fire prevention, let's also think in terms of fire detection. Most equipment rooms have actually three separate areas to consider. The first is above the ceiling, the second is the actual work area within the room, and the third is below the raised floor. Each of these locations must be considered separately when planning any type of fire detection system.

For example, smoke and particle detectors should be mounted above the ceiling, at the highest point within the room, within the work area on the ceiling, and below the raised floor, immediately under the floor. Similarly, moisture detectors also should be installed below the raised floor, where they can detect water before it becomes a disaster. Lastly, a no-smoking policy is absolutely essential within equipment areas for obvious safety concerns; it could also prevent what could be a very expensive Halon discharge should a detector be set off accidentally.

Fire extinguishers within the work area should be labeled as to their type, whether they be carbon dioxide, Halon, or whatever, as well as the type of fire they are designed to fight. Using the wrong type of fire extinguisher on a fire, particularly one involving complex equipment, could be a very, very expensive mistake, and could exacerbate your cleanup efforts considerably. There are also safety considerations involved in using the wrong type of fire extinguisher against live electrical fires.

Sources of Water in the Building

The next step in the internal evaluation of the building is to look for possible sources of water damage. Statistically, there are probably more disasters due to water in equipment areas than due to fire and other causes. There are many sources of water within a commercial building. These include obvious items such as the roof, for example, which can be prone to leaking from time to time and building plumbing including toilets, sinks, etc.; air-conditioning units are also a source of water, both in terms of the chilling water, which makes them work, and the drainage, for condensation.

Very often, drains themselves become sources of water disasters when they become clogged with insects or other debris under the floor. Sewers and other types of draining could create water disasters as well. Be sure that any type of drainage out of the building also has an approved back flow device; always remember that sewers work in reverse as well.

Speaking of this, ask yourself this question: If a water problem occurs anywhere in your building, where would the water ultimately go? Why, to the basement of course. Now think back about most of the equipment installation that you've been involved with; where do they almost invariably install the PBX? Where else? In the basement!

Often, we have no choice on where to put the PBX because telephones and utilities are considered overhead or ancillary expenses. Therefore, they are installed in places that are away from premium floor space. However, if you have anything to say about the location, especially if it's a new installation, try to seek some higher ground, and keep the PBX out of the basement.

To summarize, there are several steps one can take to avert the possibility of a water disaster. First, one very easy step is to move the floor tiles and the ceiling tiles in your equipment room, look at the pipes, and label them. For example, to a layperson looking at pipes running through a ceiling, often it is very difficult to distinguish whether a pipe is water, sewer, or electrical conduit. By labeling, when one of these pipes starts to leak, it becomes very easy in a disaster to find the shutoff quickly, thereby making it more of an inconvenience than a disaster. All this requires, really, are a couple of very inexpensive jars of paint or markers and a little

interaction with your building facilities department to find out what these pipes do.

Second, it's a very good idea to install moisture detectors under the floor, particularly in areas that are especially prone to water problems. This might be immediately under or adjacent to air-conditioning units, along major routes of water pipes that run under the floor, in low-lying areas, or it may be adjacent to drains. It's very easy to forget about what's going on under the floor, figuring that anything out of sight is also out of mind, until disaster strikes.

One last noteworthy item is to watch for any type of water pipes in areas prone to freezing. This, ironically, is more of a problem in areas such as Atlanta, Dallas, and Memphis than in areas such as Minneapolis and New York. For example, take Minneapolis in January; there is only one word for the weather! It's going to be cold. People there are acclimated to that and prepared for it. However, in the more temperate areas such as Dallas and Atlanta, very often an acute cold wave will freeze and break water pipes, which cause innumerable problems due to flooding.

While we're on the problem of changes in temperature, remember that problems can occur in the summer as well with the failure of an air-conditioning unit. Bear in mind also that just losing water service to a building could cause problems if outside water is used in your cooling systems, either for technical systems or for air-conditioners. There have been a number of reports of outages and even of companies being out of business because of a water main shutoff. This is not always the first thing we think of.

Evaluation of Electrical Power in the Building

In addition to power outages, there are a number of conditions related to power that could have a bearing on the operation of your equipment. These include items such as spikes, surges, brownouts, blackouts, noise, and any number of other types of conditions. Be sure and have the power thoroughly tested by a qualified electrician or electrical contractor prior to locating equipment.

Similarly, contact your MIS manager if you already have a data center in the building to talk about dovetailing into their UPS. It makes little sense for another manager to spend a lot of time spinning his or her wheels researching UPS systems when that expertise is probably already available in the organization in the form of the MIS manager or other technical people.

Also, during the inspection of electrical facilities, ensure that electrical cable is not run in the same conduit with telephone cable. There are two problems with this: one, it presents a safety hazard when a technician working on telephone cables that are supposed to be 48 V DC suddenly encounters 220 V or more. The second problem is the hazard of fire.

Checklist for Water-Related Disasters

- ✓ SPRINKLERS
- ✓ RESTROOMS
- ✓ "RISER" PIPES
- ✓ DRAINS
- ✓ OUTDOOR WATER
- ✓ CHILLING WATER & A/C
- ✓ ROOF
- ✓ OTHER

Lightning Exposure Checklist

Lightning Exposure to the Building — Strike One, You're Out!

- ✓ Use "gas tube" protection on telco circuits.
- ✓ Have a good solid ground.
- ✓ Don't just use a cold water pipe — insist on an earth ground circuit path.
- ✓ Keep spare IADs (integrated access devices) for VOIP telecommunications. Your router will not be grounded as your PBX is!
- ✓ Consult your electrician for other safeguards.

You will also want to check and ensure that adequate lightning protection on incoming circuits and proper grounding have been provided. One lightning strike could have devastating consequences on today's equipment. I personally experienced this when my residence was struck by lightning. The house took a direct hit on the chimney, frying some $12,000 worth of electrical equipment within the house, including satellite dishes, every phone in the house, every answering machine, every personal computer, the oven, the stove, and the list goes on and on.

There is little, if anything, that we can do about a direct lightning strike. However, there are many things we can do about indirect lightning strikes. One of the prime candidates for an indirect lightning strike are the telephone lines coming into your building; so, again, ensure that there is adequate lightning protection coming in, particularly on outside lines, to help protect your valuable equipment.

Other Prevention — Infrared Scanning

One last item you may want to consider in the electric evaluation of your building is something called infrared scan. An infrared scan uses a concept similar to the night-vision goggles, for example, that the troops wore during the Gulf War. It is

sensitive to infrared heat sources, and can show possible locations of fires before they begin. For example, the infrared scanning equipment that we've seen looks not unlike a video camera, and the equipment is used to scan the walls, ceilings, and floors in affected buildings. Any sources of heat behind the walls will show up on the infrared scan as heat sources.

Some of these are supposed to be there. For example, during a typical infrared scan, you may be going through the building with a facilities manager and see a heat source behind the wall. Upon closer scrutiny, you may find that it's simply the hot water pipe for the men's restroom, and it's supposed to be there. In other cases, it's heat, which is indicative of a problem ready to start.

One example we came across was a user who did an infrared scan of his building and found a great deal of heat coming from a breaker box. What the user found was that circuit breakers, after repeated tripping, had eventually fused themselves shut, and he was running dead shorts. This particular user is confident that the infrared scan saved his company from a very damaging fire.

Infrared scanning is available from a variety of sources. Some suggestions might be to check with the fire alarm company or the fire suppression company that your organization works with. Our recommendation is that an equipment room undergo a complete infrared scan at least on an annual basis. It ought to include the walls, ceiling, under the floor, and the equipment room, particularly if there is a lot of activity going on in the way of pulling new cable.

Safeguarding from Software Disasters through Internal Change Control

Not all disasters are caused by physical problems. Many are caused by software problems. Often, when people think in terms of software errors, they automatically think of the computer room. However, as we stated earlier, today's telecommunications equipment and routers look and act more similar to computer equipment every day, and it is every bit as vulnerable to software disasters as the computer center.

For a real nightmare, consider the effect of a software failure in the Signaling System 7 (SS7) network. Put simply, the SS7 network is the data network that tells the local and long-distance network what to do. If it were to fail because of a software failure (or virus), the results would be devastating. It has happened before. In 1990 a major telephone company made a routine software change that went wrong. The result was 150 million blocked calls — some 50 percent of this telephone company's capacity at that time. It was only the fact that this telephone company had a standard to run a full backup before major changes that saved the country from a far worse disaster. Fortunately, this particular telephone company was able to fall back to the old configuration and recover within 24 hours.

The lesson in this for all of us in the telecommunications environment is that we need a firm change control procedure when major changes are being made to PBXs

or other telecommunications equipment. If we allow these changes to be made in a haphazard fashion, when problems occur it's very difficult to retrace our steps and find out who made the changes, when, and for what purpose, etc.

There's another way to think about this, I suppose. In our family, for example, we have seven children. Because we have seven children, when I come home in the evening and something in the house is broken, nobody did it! Why did nobody do it? Because they all know that there's plenty of cover in a big family, and that I'll never be able to figure out who the offender was.

This is a kind of tongue-in-cheek reference to a problem that exists within companies, in particular, when numerous people within the technical service department have access to critical databases, and everyone is making changes. When something does go wrong, people will either not know, or not own up to the fact that they are responsible for the goof-up.

This is not to say that we should document this simply to find the responsible party, but we should limit the number of people involved in these activities to provide better training and ensure that these software-related disasters don't happen.

Formal sign-off and change control procedures for critical systems are an absolute must. Critical systems include large PBXs, Digital Cross-Connect Systems (DCS), multiplex and voice mail services, LAN servers, and other types of equipment. We'll cover some of these procedures as well as examples in greater detail later in this book.

This should be part of an ongoing process of looking for loopholes before they lead to disasters.

Evaluating the Environment with Vendors

You can work with your vendors to ensure recoverability of your network on site. First find out exactly which equipment you have on site. The vendors may have an idea of what was installed there, or you may have to refer to internal departments to determine what types of equipment was bought and when. Try and compile a list of all equipment installed on site, including the date of installation, or the approximate date if you don't know exactly when. Write down the serial number of the equipment and the revision numbers of any software or hardware associated with it. Document whether a maintenance contract is in place on the equipment, or what type of roll-in replacement guarantees you have with your vendor. Document any contractual obligations the vendor may have made in writing to support you and your system in a disaster. Outline the procedures you should follow in the event of a disaster, including escalation lists for emergency response personnel, both within the company and at the vendor's.

Lastly, work with your vendors for any type of assistance they can give you in disaster recovery planning in general. Often, the equipment vendors provide very

elaborate disaster recovery liaison programs, which can be very valuable to you in putting together a plan.

Emergency Lighting

Chances are your building already has emergency lights, but have you considered how handy it would be to have rechargeable flashlights plugged into outlets, perhaps in dark inside hallways leading to the equipment room? It sounds like a no-brainer, but you would be surprised at how many organizations skip this cost-effective precaution. Spending less than $100 at your local home improvement center will allow you to check this helpful item off your to-do list.

Main Equipment Power Breaker

If the fire department arrives at your building in an emergency, what's the first thing they do? Most people guess, "cut the power." That's a pretty good guess because that's actually the *second* thing they do. The *first* thing they do is take charge of the building. Losing control of your building raises enough issues in and of itself to write another chapter. (Just remember that in a disaster it is not your building anymore — plan accordingly; you might not be able to get back in!) As previously stated, the second thing the fire department usually does is, cut the power.

I often pose the following question to technologists (mainframe, open systems, and telecommunications managers): If someone other than you had to power down your equipment, are there not more graceful ways to do it than throwing the main breaker to the equipment? In my experience, a hard shutdown will cost you the next several days of repairing and restoring corrupted files. I know this from personal experience. Years ago I worked in a computer center for AT&T (the old AT&T). In the early 1980s, computers were rather new in the phone company. We had a computer center with about a dozen UNIX minicomputers that basically served all the testing, trouble-reporting, and administrative systems for AT&T in their former Midwest region – an area that extended roughly from Minneapolis to Mexico. In view of the fact that the incident occurred 26 years ago, I suppose the story can now be told. The names, however, have been changed to protect the culprits.

One afternoon, a fire alarm went off in the computer center when only two of us were manning it. I will refer to the other technician by the fictitious name of "Rob." This was one loud fire alarm, so loud in fact that when Rob asked, "How do you shut it off?" I barely heard him. I had one hand over my right ear and the phone on my left ear to shut out the alarm. The third time Rob yelled something at me, I thought he was asking again how to shut the alarm off. I waved him off. What he was really asking was "Is it the red button by the door?" A moment later the phone line I was on was the only thing alive in the room. Have you ever heard

the sound of a dozen minicomputers all cycling down at once in a hard shutdown? You don't want to.

Moments later there was pounding on the door (it would not open without power) and people asking us if we were ok. It took about 30 minutes for them to get the door open. By then all hell was breaking loose. They asked us what happened, and I still remember our answer to this day:

> "We don't know! The fire alarms went off and then this happened!"

Three days worth of 16- to 24-hour shifts later, while the chief system administrator and I were repairing the last of the corrupted files, I had a weak moment and told him that Rob had pressed the red button. The poor guy became "red button Rob" for the next several years, and the story has not left the computer center until now.

I can make a few other points about this story concerning disasters. If there is a responsible party, you may never find out who it was. It will be like my house with seven kids. Something is broken. Nobody did it. Much to AT&T's credit, they still deduced what must have happened and the plastic box they installed over the red button was evidence to us that they had. So what's the point to this story? It's true. It's funny. These things really do happen. What should you do in recognition of these facts?

1. How about posting the appropriate contact names and numbers prominently near the equipment room breakers? In the long run you end up the beneficiary by limiting the potential damage if somebody is tempted to do something bone-headed. You do not want to fix files for three days as we had to do.
2. There are safety concerns involved as well. When the main breaker is disconnected, many small UPS units feeding the open systems are still alive throughout the building.
2. Your building may also have a generator or backup batteries. These occasionally feed back through primary systems and can kill someone the same way a portable home generator can kill an unsuspecting lineman during a power failure. You should have a graceful shutdown procedure for both convenience and safety.

Water, Water, Everywhere: In, Over, and Under the Equipment Room

Water pipes in equipment rooms are a big deal but are rarely noticed until they leak. No one thinks of drains under the raised floor until they back up. At a minimum, you should be aware of where these pipes are, and for that matter,

what they are. (Water, sewer, gas, and electrical conduits often look alike to the untrained eye.) Know where the nearest shutoff valve is. Also, consider that with Halon falling out of use for environmental reasons, sprinklers are a fact of life these days in equipment rooms. They also leak. Consider dry pipe or pre-charged sprinklers. Then, there is the issue of water coming in from outside. Since Hurricane Katrina, everyone's perception of water entering from outside has changed.

One data services company in New Orleans reportedly took the precaution of building its equipment room on the third floor because it was in a flood-prone area. No one could have imagined floodwater over 20 ft deep. This is not a once-every-100-years phenomenon either. On December 2, 1982, a flood in Clinton, Arkansas, destroyed a central office switch. In that incident the water exceeded the 100-year flood plane level by at least 20 inches. In 1988, Hurricane Gilbert destroyed a central office switch in Shreveport, Louisiana. While on its way to Shreveport the same storm destroyed a CO in Christina, Jamaica, just for good measure. Again, in 1990 in Elba, Alabama, a levy broke (shades of New Orleans here) and caused 15.5-foot inundation downtown, which in turn resulted in 1.5 feet of water in a GTE central office equipment room — on the second floor.

I used telephone company central offices in these examples for a reason. Generally, a telephone company central office is a magnificent and robust structure because the telephone company traditionally builds a lot of the expense into the rate base. General building condition, restricted access, generators, and backup batteries, etc., are usually top of the line. Yet, look at the problems even these robust facilities have experienced. A few examples from one of our contributing authors, John Lyons, are given in the following text.

Earthquake!

In the early 1990s I was working in Simi Valley for GTE, and we experienced an earthquake at a data center there. There was minimal damage to the building, but the raised floor area equipment room sustained substantial destruction because of which the center was off the air for several days, and it was weeks before full function was restored. The reason this happened was that none of the equipment racks were anchored to the subfloor (concrete), so they were dumped over and the contents spread about the floor. Some of the equipment survived and continued to work, but many cables were severed, power was disrupted, and lots of physical damage was done.

The lesson is that in earthquake zones, it is imperative to comply with the directives while installing any equipment.

Sprinklers!

The same year in northern California, a data center had a fire protection sprinkler system that was outside the maintenance window and was erroneously triggered, thus soaking many of the libraries of backup tapes. Not only were the tapes not properly stored, but the off-site rotation schedule had been ignored; therefore, many backups were ruined and lost.

The lesson is to follow procedures for off-site rotation and waterproof the on-site storage.

Power Problem!

A couple of years later, at a network operations and monitoring center with over 100 seats and numerous dispersed customers, an overload was encountered on the UPS system because of several factors. The first was that many noncritical pieces of equipment such as radios, heaters, and non-essential machines were plugged into "orange power outlets" that were designated for UPS mission-critical equipment, including the PBX/ACD. Many of the butt-in-seat folks who were the call center staff had heard a "rumor" that orange power was somehow superior, so they moved their devices to these outlets under their desks. The load on the UPS continued to climb to near its capacity, and it climbed beyond the heat in the room where it resided. There was no temperature alarm. The rectifier board finally died from thermal overload because so many people used the room, which was small with inadequate space and airflow. It appears that what airflow that might have been available was blocked by someone using the UPS system as their personal storage for boxes and paper and anything else that was in need of tossing aside. This put the center off the air for several days as there was no alternative power source for the switch, although some of the network tools came online after some juggling of power plugs.

No one was assigned to the UPS, no alternative source was available for the PBX/ACD, and numerous devices were running on it unnecessarily. I became the HVAC/power/UPS person after that ordeal. It was fortunate that there was no fire. We had more than a few customers who were not happy before this incident, and after the repairs were made, several left for other companies.

This center was moved from InfoMart on Stemmons Freeway in Dallas, Texas, and there were difficulties from the first day of operations. LAN wiring was not properly terminated, labeled, or run to all locations. The patch panel closet had been a mop closet and was so small as to be impossible to move about without knocking something loose. The place reminded me of what was called the wine cellar on a B52, although I was a much younger person and much more agile in the days when I crawled around in that small place.

Software Error!

We had many other funny and interesting times. A set of software operating system patches were installed on an operational server in Sacramento by some folks in Tampa without first doing any regression testing. That dumped the application and the sysplex had to be rebuilt, which was a week-long event. Change management procedures were ignored, and this led to many difficulties, including network routing issues that left whole segments of the country unable to access these applications.

On another occasion I was dispatched to Fort Wayne on a "crit sit," or critical situation. An $8 million sale hinged on getting two servers operational that had not been turned up successfully. The supposed fix was a set of patches coded in Edinburg, Scotland, and sent by FTP (File Transfer Protocol) to a server there. After some difficulty, because of the 6-hour difference in time zones and my working in the wee hours of the morning, I managed to get the code needed for the repair to my laptop. The interface to the server required an unusual (read scarce) SCSI cable, and the only one available was in New York, thus necessitating a counter-to-counter shipment via American Airlines. Once this was completed, the connection (external) to the server was made. These were HP 9000 servers sealed at the factory in Scotland after their custom hardware and software was installed. We were forbidden to open the hardware because it was under warranty and, likely, turf wars between the U.S. and our Scottish cousins. With all this, I still could not get the server to respond. I finally opened the box (without permission) and discovered that the cable from the external SCSI connector to the motherboard had been removed. The Scottish version was that this was done to meet Network Equipment Building System (NEBS) compliance, but methinks that it was done to obstruct our access.

We could not get a complete new box shipped for at least three weeks because of customs and other constraints on international trade. I fixed it by installing the internal cable and loading the software. Needless to say, we did not make the dates, but the sale eventually was completed.

Where Is Your PBX?

Before we leave the subject of floods, consider where most of your telecommunications equipment probably is. I'll give you a hint — It reminds one of an old Rodney Dangerfield joke: *"I don't get no respect. When I get in an elevator, the people look at me and always say the same thing — basement?"*

Telecom managers apparently have the same problems with respect because, often, that is precisely where the PBX or fiber-optic equipment goes — in the basement. The second choice? Riser closets, as we just discussed. Bad choice. Riser closets mean that if there is any water problem in the building (and invariably pipes are in the risers too, as the previous example shows), the water runs down to your

equipment. Interestingly enough, fiber optics will operate immersed in water; the electronics that powers the fiber regrettably will not.

Ultimately, enough water anywhere in the building will end up in the basement, and usually right down the risers. To mitigate some of the risk, check to see if your risers are adequately fire-stopped with approved material around all floor penetrations. Try to avoid steel grid flooring in the risers if possible. It gives you some protection not only against fire, but water as well.

Physical Access to Equipment Rooms

Notwithstanding hurricanes and floods, people cause most disasters. For those of you who underestimate this issue, consider the following true story, again from someone who lived it firsthand — me.

About five years ago, when I was CEO of a telecommunications firm (and as luck would have it, on the day our chairman of the Board was visiting), we were in the process of installing a Class 5 telephone switch. One component of the installation was a large bank of 48-V batteries.

Immediately after completing the installation, my switch room manager left for lunch, with strict instructions to his two helpers: "Don't touch anything."

Fifteen minutes later, my director of operations burst into my meeting with the chairman, saying that something had gone terribly wrong. There had, by initial indications, been a battery explosion. The building was being evacuated. My chairman gracefully ended the meeting and left, while I headed to the equipment room.

I learned that the two subordinates had never worked on a negative 48-V system (very common in telco environments). Even so, after the supervisor left they had been discussing why the positive (+) side of the equipment could have a black wire and how the negative (–) side could have a red wire. After some discussion (even though the equipment was operating that way), the two resolved to remove the wires and put them on the "right" way; in the process they turned the wires into a 300-A arc welder.

The batteries didn't explode, but every wire fried instantly and completely filled the first floor of this multi-tenant building with smoke. This caused the evacuation of all floors. Not only us, but also all the other companies in the building spent the afternoon in the parking lot. Then the fire department arrived. Guess who got to be the spokesperson! Fortunately, nobody was hurt as a result of the incident.

The story ends with several of us executives (including coauthor Dave Mowery who wrote the Sarbanes–Oxley section of this book) defusing the public relations nightmare by making a donation to the local fire department for new infrared scanning equipment. (After all, it sees through smoke, right?) The funniest part was seeing our picture in the local DeSoto, Texas, newspaper with a big cardboard check; model citizens to everyone reading the paper, but boneheads to everyone

who knew what really happened. I have not even gotten to the punch line of this little adventure yet.

One of the technicians switching the wires was none other than my son-in-law. Jason was aptly christened "Sparky," and he will wear that name probably until the day he dies. In the world of telecommunications, Mr. Murphy (who coined the phrase "if it can go wrong it will") was an optimist. Lesson here: Keep your eyes open, and monitor your employees and contractors.

One way to avoid these kinds of problems is to monitor who goes in and out of the equipment room. Do you restrict access to these areas to people who absolutely must be in there? What about where you locate your equipment room? Does your organization, God forbid, still put servers in janitor's closets? If so, how is the airflow in that cramped closet, which is your server room? Do the doors lock to your equipment areas? Do you store large piles of paper or combustibles with your equipment? What about under the floor, where the night shift employees hide their cigarettes? Pop a floor tile and look under there. Does it look like my teenager's bedroom?

Don't forget to look at another big cause of people-related problems: "routine" system software changes. Every system (that means mainframe, telecom, and LAN) should have a formal well-documented change control procedure, defining not only how, but also who should make changes that could potentially affect continuity of service.

Backup –48 V Power for Telecommunications Equipment

Notwithstanding my amusing personal story in the preceding text, one of the most critical items to consider is the lack of some type of –48 V backup power for Digital Access Cross-Connect Systems (DACS) fiber-optic transmission equipment, switches, muxes, and other telecommunications equipment. Although they don't realize it, many companies today have crossed the invisible boundary between being a large corporate user and being a service provider in and of themselves. As such, an organization may be on a learning curve as to which standards and procedures are appropriate for what is now a central office. Standards for –48 V backup power are one concern. If your organization has a large PBX and has assumed the role of de facto phone company, you are a candidate to adopt telco-grade standards. Don't assume UPSs will be enough. UPS systems fail, too; I have seen that happen firsthand. Phone companies use batteries, and so should you.

Using the State Public Utility Commission Information for Disaster Recovery

A wealth of information can be obtained at little or no cost by visiting the Public Utility Commission (PUC) for your state. Much of the information filed in state

PUCs is technically public domain and available to anyone with the initiative to go after it.

One type of information on file with state PUCs is the definition of serving central office areas, often right down to the foot. This could be important information in evaluating how difficult or expensive it may be for your company, for example, to build diverse facilities to a separate serving office. With this information, you'll also find the definition of exchange boundaries and calling scopes. Although often not a primary concern for companies, local calling areas can be an important consideration in how much future business costs.

There will also be information on distances to other central offices. This is extremely important if your company is considering any type of diverse access to other serving wire centers. There will also be information on central office upgrades and central office capacity.

To summarize, a visit to your state PUC could provide both an interesting perspective into and valuable information for your Disaster Recovery Plan. It's well worth taking a one-day short trip to Albany, Austin, or San Francisco to see what valuable information may be available.

CHAPTER 5
WORKSHEETS

WORKSHEET No. 1

Operating Standards Checklist

This is by no means a comprehensive list, but you can flesh it out with ideas from the chapter, and your organization's own experience and policy.

Yes	*No*	
		Do walls extend from floor to ceiling, both above suspended ceilings and below raised floors?
		Are all wall and floor penetration fire-stopped with approved material?
		Are fire-resistant cables installed in all plenum (airflow) areas?
		Is a no-smoking policy enforced?
		Is commercial power tested for spikes, surges, brownouts?
		Is there UPS for all "top ten" mission-critical systems?
		Is equipment secured from theft?
		Is there card-key access to equipment areas?
		Are sign-in procedures in place?
		Is janitorial staff in equipment closets?
		Do you know where telephone cables come into your building?
		Do cable vaults have fire protection?
		If below grade, do cable vaults have water protection or drains?
		Does the building have a generator and test schedule?
		Are all water shut-off valves properly and easily identified?
		Are all critical electrical breakers properly identified?
		Is Halon in use?
		Are dry pipe or pre-charged sprinklers in use over equipment? If not:
		Are plastic sheets or covers immediately available?
		Are numbers for professional recovery companies such as BMS Catastrophe posted?

WORKSHEET No. 2

Operating Standards Checklist

What is the general condition of the equipment room?
(5 = Excellent 4 3 2 1 = Poor)

	5	*4*	*3*	*2*	*1*
Management of combustibles					
Access					
Temperature variation					
Airflow					
Above ceiling					
Below floor					
Drains/water detection					

WORKSHEET No. 3

Security Standards Checklist

This is by no means a comprehensive list, but you can flesh it out with ideas from the chapter and your organization's own experience and policy.

Yes	*No*	
		Does a written policy exist for disposal of confidential materials?
		Does a written policy exist on communications privacy?
		Is there a policy for telecommunications restoration priority (mission-critical 800 numbers first, for example)?
		Are backups regularly performed on:
		Mainframes
		"Open system" servers
		Bridges, routers, gateways, switches
		PBX
		Does the organization have a written Operational and Security Standards document?
		Does a parcel pass system exist to prevent theft?
		Is a documented change control procedure in place for all equipment that can impact "top ten" business applications identified in the Chapter 1 worksheets?

What is the general level of documentation existing right now regarding:
(5 = Excellent 4 3 2 1 = Poor)

	5	*4*	*3*	*2*	*1*
Change control					
Standards					
Disaster Recovery Plan					

Chapter 6

Documenting the Plan — What to Include

Leo A. Wrobel

Contents

Why Document It at All? 133
Developing an Equipment Inventory 134
Putting the Disaster Recovery Plan to Paper 143
What Should the Plan Cover? 150
Recovery Scenarios — The Three "R's" 152
Summary 163
Chapter 6 Worksheets 165

Why Document It at All?

Often, a technical services organization's response will be cold when asked to produce a disaster recovery plan. The idea in the mind of technical service persons is that management does not trust them to do their job in the event of a disaster. They can sometimes even look at the disaster recovery plan as some kind of a test to prove that they know how to do their jobs! This is certainly not the case. Virtually every organization that I personally have had the opportunity to work with is capable of recovering from a disaster under any type of circumstance. This may sound like a very surprising statement. In most large organizations the technical service staff are the persons most capable of recovering from many types of outages. Often, the very people controlling the recovery process are those who actually designed and built the system in the first place. Technicians usually know where every wire runs in the organization. Programmers are quite familiar with the internal workings of the

equipment, and anyone with day-to-day operational responsibilities probably has major vendor and supplier telephone numbers committed to memory.

All of these departments usually pull together in a superhuman effort to respond to a disaster with remarkable success. So, if this is the case, then what's the problem?

The problem centers chiefly around what happens to the response to a telecommunications disaster when key personnel are either incapacitated by the disaster, don't show up for work, or are otherwise lost. One of my favorite ways to check the disaster recovery plan is to come into an organization, assemble the disaster response team, and at the beginning of the test, point around the room and say, "You, you, and you! You're dead!" And then, see how the organization responds to the test. Sometimes, I try not to be so morbid. I point around the room and say, "You, you, and you! You are all vacationing in Fiji on the beach, and there are no telephones!" This conjures up a nicer mental image.

The point that I am making is what happens to an organization's response when key people are not available in a disaster?

Therefore, the goal of the organization should be to document the Disaster Recovery Plan in a format that can be followed by any reasonably trained technical service person. For example, a vendor, a rental tech, a major supplier, a carrier company, or other resource; someone with reasonable technical training who could follow a systematically organized plan to help the organization recover, should be able to understand the plan.

In light of these thoughts, it is important that you present disaster recovery to your staff, not as some type of a quiz or test to prove that they know their job but to portray a realistic scenario that someone other than they may be called to execute this plan.

As the person or persons controlling the recovery process may not be familiar with the organization, it is essential that everything be documented in a format designed to be easily followed by a technical person supporting the recovery efforts. For example, use a lot of pictures and diagrams. We'll talk about this as we get further into the chapter.

Developing an Equipment Inventory

One of the items that will be required in the recovery plan is an equipment inventory. It's important for the people coordinating the recovery and response to know what was installed, not only the type of equipment but also software packages, for example, which reside on the equipment. The inventory should also include equipment model numbers, software revision numbers, date of purchase, original cost of the equipment, critical rating, and power requirements for the equipment. Other items could also be included, such as the name, address, and telephone number of both the manufacturer and the distributor of the equipment. The equipment inventory may include an amortization schedule for the equipment (see the following diagram).

Sample Equipment Inventory Form

Equipment:

Manufacturer:

Serial Number:

Software Version:

Purpose:

Criticality Rating (1, 2, 3, 4):

Date of Purchase:

Remarks:

If the equipment is depreciated over a five-year life and is now four years old, the decision may be to simply replace rather than repair the equipment, as much of its useful life has already been expended. This form can be important to have at a time when many command decisions regarding replacement of the equipment will have to be made by someone in very rapid succession. The more information on hand in a digestible format to provide a rationale for these decisions, the better for the company and for the decision maker.

Other items should also be contained in an equipment inventory. For instance, a separate inventory should be maintained of all equipment residing at a disaster recovery center. It should get down to some fairly minute details as well. Do you know whether the equipment is on a rollable rack, which could be moved off of the floor quickly, or will it require dollies? What physical types of power plug does the equipment use, etc.?

"Importing" Data to Ensure Accuracy

The best method for keeping track of equipment necessary for the recovery process is through a procedure called "importing" data. We will stress this concept of "importing" data repeatedly through this section. What "importing" data essentially means is finding databases and repositories of information within the

organization which you can reasonably expect to stay up to date, then pulling them into the plan on an automated basis.

For example, when a piece of equipment is purchased, a document or file for the equipment is archived somewhere within the organization. The location varies from organization to organization. Sometimes, the contract and the documentation to the equipment go to an accounting department where it is put away to be amortized. Sometimes, the files are stored on a network. Sometimes, the files become part of the personal file of a manager or analyst's personal papers. The key is to locate and identify these repositories of equipment inventory data so they can be imported gracefully into the recovery plan.

There are a number of good reasons for taking this approach. First, equipment is often purchased with roll-in replacement guarantees or maintenance contracts. A savvy technical service manager may negotiate a contract for a new high-end server with a vendor. As part of the contract, the vendor would agree to have another server of similar capabilities and capacity available within 24 hours of the disaster.

If this information were not imported into the recovery plan, it would be very easy, given the turnover of personnel in many organizations, for this information to be forgotten later on. Someone down the road may find the need for a disaster recovery plan for the same server and pay extra money on a component, which already has a roll-in replacement guarantee to begin with. That is duplicative, wasteful, and unnecessary.

Organizations that make heavy use of LANs could possibly have an obvious advantage in importing data. In a paperless environment, it becomes relatively straightforward to import data from other files, and perhaps even other departments connected to the same LAN. There are numerous ways in which this could be automatically transferred without human intervention to a critical file within the recovery plan. One way would be by using object-linking Microsoft Word files every time a file is updated in the accounting department showing the purchase of a new piece of equipment. (See Figures 6.1–6.3.)

By keying in on a specific file name, for example, a file in the accounting department, a technical service manager can be assured that every time that department updates an equipment list in accounting, the file in his recovery plan will also be similarly updated. For more information on this type of object-linking, consult your Microsoft Word user manual, or check out similar functionality with the word processor your company uses.

Other Inventory Items

Other items that may find a useful place in an equipment inventory include the location and phone numbers of secondary market equipment suppliers. Very often, these suppliers are instrumental in locating equipment (particularly equipment that

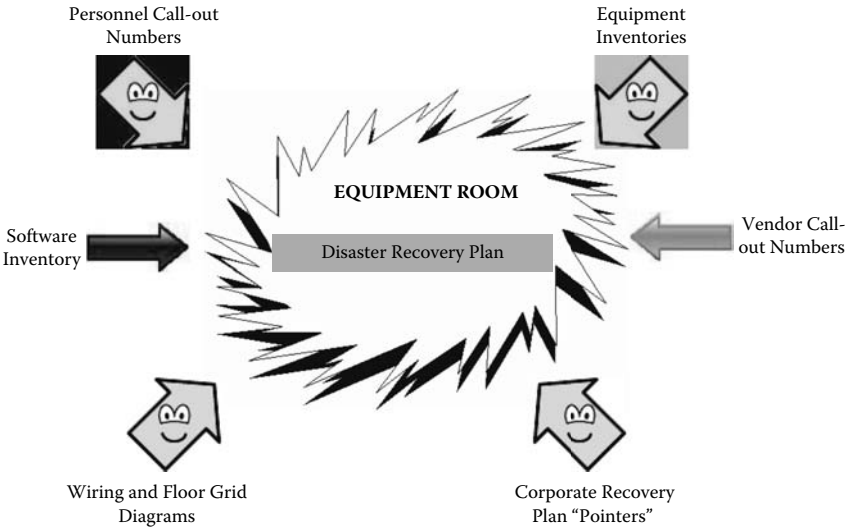


Figure 6.1 Disaster recovery plan: equipment room.

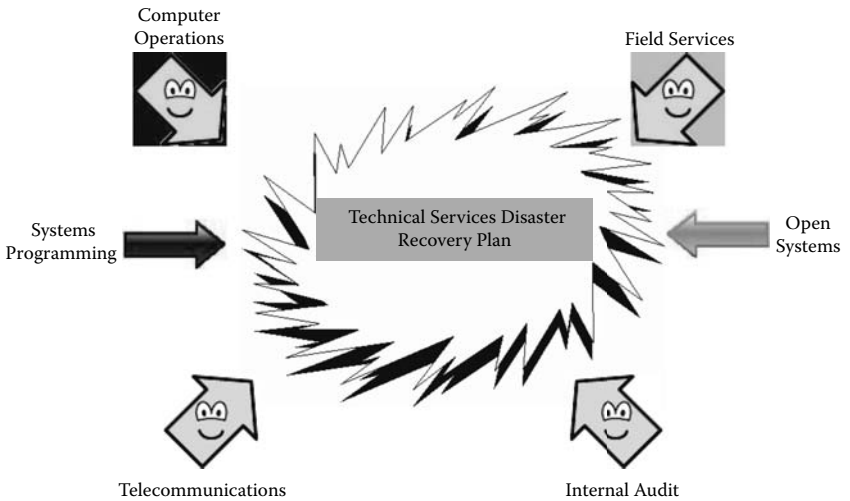


Figure 6.2 Technical services disaster recovery plan.

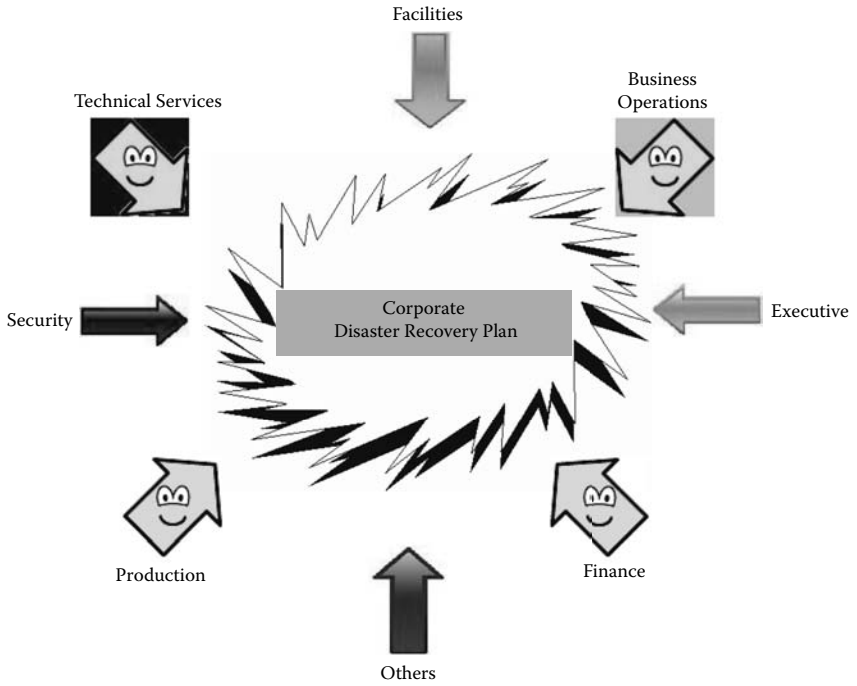


Figure 6.3 Corporate disaster recovery plan.

is a couple of years old) in the event of a disaster, as much of it may already be seeing activity on the secondary market.

Roll-In Equipment Replacements

While we're on the subject of equipment replacements, let's talk for a moment about roll-in replacements. Given the price of some of today's technical equipment, it's not unreasonable at all to use disaster recovery in the selection criteria for major equipment purchases.

As any mission-critical piece of equipment should have a disaster recovery plan, it behooves us all to try to obtain this recovery plan from the vendor first. Such equipment should include high-end servers, automated call distribution units, PBXs, major bridges, routers, and gateways and LAN networks, as well as mainframe computers. For equipment vendors, disaster recovery programs could be just the edge they need to add value to their services and secure very lucrative contracts with users. In any event, it is much more cost effective to try to negotiate disaster recovery services with a vendor while they are vying for your business and hungry for your business rather than trying to add these services later.

More and more equipment vendors are offering rapid replacement services, particularly for big-ticket items. Even suppliers of smaller equipment are finding that providing the value-added inherent services in disaster recovery gives an edge over competition and may help secure a sale. Therefore, it makes sense to check with all equipment vendors to determine what types of programs are available.

Maintaining the Inventory

To develop and maintain an equipment inventory, seek out accurate repositories of equipment inventory data. Second, import from these sources whenever possible to ensure accuracy. Importing can be accomplished via a LAN in optimal situations, but it can also be accomplished by simply assigning responsibility to a key person or division to go to that department on a regular basis to make a CD-ROM (compact disc read-only memory) copy of the appropriate file. This person will also be responsible for updating the recovery plan.

If the latter option is chosen, it is important to put some teeth into it to ensure that it gets done. For example, if John Smith is responsible for copying the equipment inventory file for the Disaster Recovery Plan and fails to get this done, he might not be eligible for a raise next time around. In a busy operational environment, it is often necessary to take these steps to demonstrate importance to the recovery planning process. Without these steps, it becomes all too easy for busy technologists to simply fail to update the plan, guaranteeing that it will be out of date when needed.

Using Vendors to Help with the Inventory and Plan

Lastly, try and get all the mileage you can from vendors before opting for expensive equipment replacement programs. This, again, is best accomplished when the vendor is knocking at your door trying to do business and not adding disaster later as an ancillary service after the equipment has been purchased.

Maintaining Other Information by Importing

Because maintaining up-to-date telephone numbers for personnel and critical equipment vendors is absolutely essential to the successful implementation of the plan, similar methodology must be employed to ensure accuracy. Once again, this means importing data from known reliable sources.

Let's consider wireless and home telephone numbers of employees. There are many places within the organization one can go to find these numbers for key employees. Places include Human Resources, the company telephone directory, and other repositories.

Depending on the company, Human Resources may be the best place to get this information. However, we have seen companies where even the information in Human Resources is ridiculously out of date. A key employee who has worked for the company for 20 years, for example, may go to Human Resources and find that the address on file is the one he had 20 years ago when he was hired. Similarly, the company telephone directory, if one is available, may be a good repository of data. Often the documents are only published annually and quickly become out of date.

Once again, the key to success in this area lies in identifying accurate repositories of telephone number data and importing them into the recovery plan. Once again, this is best achieved through object-linking files together, perhaps in a LAN environment. It can also be accomplished through use of a sneakernet (the process of sharing files by copying them onto floppy disks or tape and actually physically handing it to another user) and CD-Rom. The important thing is that it be done regularly, and preferably, without manual human intervention.

Other numbers that will be needed are the telephone numbers of key equipment vendors and suppliers. Often these can be found in the Network Control Center, help desk, or other operational environment with day-to-day contact with these vendors. A good rule of thumb would be to import vendor call-out data from these operational environments. When telephone numbers for key vendors and suppliers change, these people are the first to know. Also, because they're usually involved in escalation procedures on a regular basis, it's a good bet that second- and third-level management within the vendor community would also be documented in these departments.

A third item that should be rigorously defined in the telecommunications recovery plan is the circuit inventory. This can come from a number of sources, including a circuit analysis department, a telecom analyst who is responsible for ordering these circuits, the Network Control Center, and often today, even from circuit call records contained inside intelligent multiplexers.

Some intelligent multiplexers in the telecommunications environment provide for data dumps of all circuit "calls" established within the multiplexer. This provides for quick and easy reestablishment of these circuits through a CD or DVD copy or a manual process from a printed record, either of which can be safely stored off-site until disaster strikes.

It is important to take regular backups of this data contained within the multiplexers and have it included in the regular pickup schedule for magnetic media for the data center. This should be accomplished at least weekly or much more often, such as maybe daily, in very intensive operations that change rapidly.

Other items that should be included in the circuit inventory might contain the corresponding logical assignments within IBM front-end processors or routing tables in major routers. Although this type of information is really the responsibility of other systems personnel outside of telecommunications, having the information on hand provides for a graceful flow when it's time to implement the plan.

Importing or Developing a Software Inventory

Another item to consider is the software inventory, encompassing all software required for operation of all mission-critical equipment. This inventory should include the acquisition date of the software, the original cost of the software, the license number, and the version number. In fact, pay particular attention to software versions. Getting too many generations, or too far out of date on software and hardware versions, is an open invitation to problems in a disaster when the version of the software you are running may no longer be available. This could cause significant delays in the recovery process. The software should be backed up regularly and stored off site, possibly being picked up along with the MIS or LAN manager's regular software pickup schedule. The following example illustrates a basic software inventory form.

Including Floor Grid Diagrams

A fifth item to be considered, and again possibly imported, includes floor grid diagrams. These diagrams should show all installed equipment for the effective equipment room, and delineate any special environmental specifications such as airflow,

Sample Telecom Software Inventory Form

Software Package: _____

Vendor: _____

License Number: _____

Software Version: _____

Purpose: _____

Criticality Rating (1, 2, 3, 4): _____

Date of Purchase: _____

Remarks:

temperature, special power, special power plug, etc. They should also outline equipment footprints, clearances, and any other information that would be of use to an installer setting up one of these items.

Importing Components of the Corporatewide Plan

One final item to consider would be the introduction or the importing of selected components of the Corporatewide Recovery Plan. As we stated earlier, it makes little sense for the Telecommunications Recovery Planner to write procedures for such broad-based concerns as loss of a building, physical security, fire procedures, bomb threats, and other items that are more global in nature than telecommunications specific.

In these cases, the Telecommunications Recovery Planner should use pointers directing the reader of the Telecommunications Recovery Plan to the relevant section of the corporate plan for such broad-based concerns. Indeed, as far as the makeup of the recovery plan is concerned, the telecommunications recovery plan itself may, in fact, end up being imported into a Corporatewide Recovery Plan for execution by an emergency management team.

The Corporatewide Recovery Plan covers a whole host of broad-based disaster recovery issues. This document would include subsections from a Technical Services Recovery Plan, a Facilities Recovery Plan, Business Operations Recovery Plan for actual logistical day-to-day business, and Executive Recovery Plan, or procedures for an Executive Management Team. It might also have sections from Security, Production, and Finance. A Technical Service Recovery Plan on the other hand embodies all technical service departments for inclusion in the Corporatewide Recovery Plan. These would include departments such as computer operations, systems programming, field services or outside installation personnel, and distributive processing, such as LANs. There would also be input from the internal audit department and, lastly, telecommunications, which would become one component of a Companywide Technical Services Recovery Plan.

One can even split the Telecommunications Recovery Plan into numerous subsections, including Voice Communications, Data Communications, and the Network Control Center Recovery Plan.

For example, a network control center or help desk could take on a very different meaning in a disaster situation by helping to maintain command and control. Network engineering may have its own section of the Disaster Recovery Plan, as well as telecommunications field service personnel and telecommunications operations personnel.

All of these various telecommunications departments will be defined in the recovery plan. Each has assigned day-to-day responsibilities and, correspondingly, each will be assigned specific responsibilities during a disaster.

Summary

To summarize, the Disaster Recovery Plan is a complex road map on how to rebuild your organization after a disaster. Optimally, it should be written for a reasonably well-educated technical person to execute in the event key personnel are incapacitated or unavailable after a disaster. It includes input from all major vendors, suppliers, and departments, and must import data from known accurate sources to be a worthwhile document in time of disaster. We will explore the makeup and contents of this document in the coming chapters.

Putting the Disaster Recovery Plan to Paper

As we stated earlier in the book, the principal reason for carefully documenting the Disaster Recovery Plan is to allow for the recovery of critical technical systems in the event the persons normally responsible for those are incapacitated or unavailable as a result of the disaster. This requires laying out disaster recovery tasks in an understandable and systematic format. Diagram No. 6A illustrates such an approach. The diagram was compiled from a number of disaster recovery plans written for real-life companies. It represents a kind of middle-of-the-road approach to recovery planning.

Diagram No. 6A

Sample Disaster Recovery Plan Table of Contents

Section I Policy Statement
- A. Objectives of the Project — Overriding Themes
  1. Protect lives
  2. Minimize risk to your organization
  3. Recover critical operations
  4. Protect against lawsuits
  5. Preserve competitive position
  6. Maintain customer confidence and goodwill
  7. Synopsis of preliminary BIA and recovery strategy

Section II Overview of Recovery Scenarios
- A. Initial Reaction Procedures to a Disaster Report
  1. Notification of police, fire, and medical
  2. Notification of management
  3. Mitigating the cause
  4. Filing of initial damage assessment reports
  5. Providing security at the affected facility

B. Business Resumption Overview
   1. Activation of Emergency Management Team (EMT)
   2. Activation of disaster teams
   3. Activation of backup plans
   4. Decision to declare a disaster
   5. Decision to activate recovery center
   6. Relocation to recovery center
   7. Coordination with local authorities
   8. Notification of customers, financial lenders, and media
   9. Activation of the recovery center equipment

C. Damage Assessment Overview
   1. Coordinating with EMT
      - Responsibilities of EMT
      - When to notify EMT
   2. Notification of EMT
      - How to notify EMT
      - Support services required by EMT
   3. Reports to EMT
      - Format of reports
      - Frequency of reports
      - Format and procedure for initial reports
   4. Notification of clean-up companies
      - Responsibilities
   5. Interfacing with local authorities
      - Responsibilities

D. Other Recovery Activities
   1. Assisting EMT in preparation of official statements
   2. Opening a critical events log
   3. Modified signing authority
   4. Where to get cash
   5. Physical security
   6. Security at the damaged site
   7. Security at the recovery center
   8. Security at emergency funds disbursement centers

E. Restoration of Critical Business Functions
   1. Coordination of restoration of the original site
   2. Restoration of hardware systems
   3. Restoration of software systems
   4. Restoration of power
   5. Replacement of fire suppression systems
   6. Adding security
   7. Rewiring of the facility
   8. Restoring the networks

9. Testing new hardware
10. Coordinating return to original site
11. Scheduling migration back to original site

III. Technical Services Department-Specific Recovery Procedures

A. Companywide Disaster

1. Loss of a building or data center
   - Receive initial report
   - Notify EMT and staff
   - Initial damage assessment
   - Safeguard human life
   - Coordination of emergency services
   - Help for the injured
   - Restoration of network control help number
   - Restoration of help desk incoming numbers
   - Command routing of incoming 800 service
   - Remote call forwarding of local telephone service
   - Redirection of backbone T1 network
   - Redirection of critical LAN router links
1. Fire
   - Receive initial report
   - Notify EMT and staff
   - Initial damage assessment
   - Safeguard human life
   - Coordination of emergency services
   - Help for the injured
2. Flood
   - Receive initial report
   - Notify EMT and staff
   - Initial damage assessment
   - Safeguard human life
   - Coordination of emergency services
   - Help for the injured
3. Earthquake
   - Receive initial report
   - Notify EMT and staff
   - Initial damage assessment
   - Safeguard human life
   - Coordination of emergency services
   - Help for the injured
4. Tornado
   - Receive initial report
   - Notify EMT and staff
   - Initial damage assessment

- Safeguard human life
- Coordination of emergency services
- Help for the injured

5. Sabotage/Vandalism
   - Receive initial report
   - Notify EMT and staff
   - Initial damage assessment
   - Safeguard human life
   - Coordination of emergency services
   - Help for the injured
6. Bomb Threat
   - Receive initial report
   - Notify EMT and staff
   - Initial damage assessment
   - Safeguard human life
   - Coordination of emergency services
   - Help for the injured
7. Power Loss
   - Receive initial report
   - Notify EMT and staff
   - Initial damage assessment
   - Safeguard human life
   - Coordination of emergency services
   - Help for the injured
8. Security Breach
   - Receive initial report
   - Notify EMT and staff
   - Initial damage assessment
   - Safeguard human life
   - Coordination of emergency services
   - Help for the injured

B. Telecommunications Emergency Procedures — Telecommunications Disaster

1. PBX, ACD, or Voice Mail System Hardware Failure
   - Determine nature of disaster
   - Determine extent of disaster
   - Determine cause of disaster
   - Secure the installation
   - Notification of Telecommunications Manager
   - Notification of principal vendors
   - Notification of EMT
   - Assembly of Telecom Recovery Team
2. PBX, ACD, or Voice Mail System Software Failure

- Determine nature of disaster
- Determine extent of disaster
- Determine cause of disaster
- Attempt to recover via backup software copy
- Procedures for virus infection
- Procedures for hacker attack/unauthorized intrusion
- Notification of Telecommunications Manager
- Notification of principal vendors
- Notification of EMT
- Assembly of Telecom Recovery Team

3. Major Cable Cut (Extended Outage)
   - Determine location of cable cut
   - Determine extent of disaster
   - Determine cause of disaster
   - Escalate problem with the vendor
   - Notification of Telecommunications Manager
   - Notification and status reports to critical users
   - When to notify the EMT
   - When to assemble the Telecom Recovery Team
   - When to activate a Telecom Recovery Plan
4. Failure of Major T1 Node
   - Determine nature of disaster
   - Determine extent of disaster
   - Determine cause of disaster
   - Secure the installation
   - Notification of Telecommunications Manager
   - Notification of principal vendors
   - Notification of EMT
   - Assembly of Telecom Recovery Team
5. Failure of Major Front-End Processor
   - Determine nature of disaster
   - Determine extent of disaster
   - Secure the Installation
   - Notification of Telecommunications Manager
   - Notification of principal vendors
   - Notification of EMT
   - Assembly of Telecom Recovery Team
6. Loss of Critical Bridge/Router/Gateway
   - Determine nature of disaster
   - Determine extent of disaster
   - Determine cause of disaster
   - Secure the installation
   - Notification of Telecommunications and LAN Managers

- Notification of principal vendors
- Notification of EMT
- Assembly of Telecom Recovery Team

7. Loss of Bell Operating Company Central Office
   - Determine extent of disaster
   - Determine cause of disaster
   - Escalate problem with the vendor
   - Notification of Telecommunications Manager
   - Notification and status reports to critical users
   - Notify the EMT
   - Assemble the Telecom Recovery Team
   - Activate a Telecom Recovery Plan
   - Follow EMT Instructions in corporate recovery effort
   - Provide timely reports to EMT on status
8. Loss of AT&T (Or Principal Long Distance Carrier)
   - Determine extent of disaster
   - Determine cause of disaster
   - Escalate problem with the vendor
   - Notification of Telecommunications Manager
   - Notification and status reports to critical users
   - Notify the EMT
   - Assemble the Telecom Recovery Team
   - Activate a Telecom Recovery Plan
   - Activate 800 Command Routing features
   - Provide timely reports to EMT on status
9. Power Surge
   - Determine extent of damage
   - Determine cause of disaster
   - Determine affected equipment
   - Secure the installation
   - Notification of Telecommunications Manager
   - Notification of principal vendors for affected equipment
   - Notification of EMT
   - Assembly of Telecom Recovery Team
10. Lightning Strike
    - Determine extent of damage
    - Determine cause of disaster
    - Determine affected equipment
    - Secure the installation
    - Notification of Telecommunications Manager
    - Notification of facilities manager
    - Notification of insurance carrier
    - Notification of principal vendors for affected equipment

- Notification of EMT
- Assembly of Telecom Recovery Team

11. Theft of Equipment
    - Determine nature of the theft
    - Determine affected equipment
    - Secure the installation
    - Notification of security
    - Notification of Telecommunications Manager
    - Notification of facilities manager
    - Notification of insurance carrier
    - Notification of principal vendors for affected equipment
    - Notification of EMT
    - Assembly of Telecom Recovery Team

C. Wrap-Up Activities
1. Review of Critical Events Log
2. Evaluation of vendor performance
3. Recognition of extraordinary achievements
4. Preparing Final Review and Activity Report
5. Aid in liability assessments
6. Schedule compensatory time off

Section IV Testing and Maintenance of the Telecommunications Plan

A. Testing Procedures
1. Affected departments
2. Responsibilities
3. Reference documents
4. Frequency of testing
5. Pretest coordination
6. Scheduled tests
7. Unscheduled tests
8. Introduction of complications
9. Evaluation of results

B. Telecom Plan Maintenance Procedures
1. Affected departments
2. Responsible personnel
3. Frequency
4. Hardware change procedures
5. Software change procedures
6. Staff or team member changes
7. Vendor list updates
8. New technologies or equipment
9. Contract renewals
10. Emergency assistance changes

Section V Telecom Disaster Recovery Training
A. Training Procedures
1. Scope of training
2. Affected departments
3. Responsibilities
4. Reference documents
5. Frequency of training
6. Required versus optional training
7. Media to be used
8. Specialty team training
9. General new hire training

Section VI Appendices to the Telecom-Department-Specific Recovery Plan
Appendix 1 Emergency Call Lists of Management and Recovery Teams
Appendix 2 Vendor Callout and Escalation Lists
Appendix 3 Inventory and Report Forms
Appendix 4 Carrier Callout and Escalation Lists
Appendix 5 Maintenance Forms
Appendix 6 Hardware Lists and Serial Numbers
Appendix 7 Software Lists and License Numbers
Appendix 8 Team Member Duties and Responsibilities
Appendix 9 Network Schematic Diagrams
Appendix 10 Equipment Room Floor Grid Diagrams
Appendix 11 Contract and Maintenance Agreements
Appendix 12 Special Operating Instructions for Sensitive Equipment
Appendix 13 Wireless Phone Inventory and Agreements
Appendix 14 All Other

What Should the Plan Cover?

The first question you should ask is, "What should your Disaster Recovery Plan cover?" For example, does your company store food on site? Often, while lecturing on the East Coast, I draw a lot of smiles and laughter when I ask this question during lectures. On the West Coast, however, with the ever-present threat of earthquakes, companies do, indeed, store food on site.

I've seen recovery plans with sections on: "What do you do with an employee who freaks at the sight of a dead body? What do you do with a dead body if you're stuck in the building with it for a number of days?" Once again, this is not to be morbid, but statements such as these do often occur in recovery plans for companies in earthquake- or other disaster-prone areas.

After deciding the types of topics to be covered by the plan, we must also decide the depth, or level of detail, that we'll cover in the plan. I prefer the "Lewis and Clark" approach. Pack only enough to be able to live off the land and survive the trip. Remember, if you pack two of everything just in case, you double your costs. Better to have the equivalent of a good knife and some fishhooks. Think of the things you will need as a technologist to "live off the land" post disaster. You also will not burden the plan with too much detail. By providing too much detail, the plan becomes difficult to follow, particularly by people not employed by the company. It also becomes extremely bulky and imposing, discouraging people from really reading and understanding it. A more precisely written recovery plan is just fine if the recovery is conducted by employees who are familiar with the equipment configuration. Once again, it could be very difficult for outside employees to handle the recovery.

Now that we've discussed these items, let's move into the actual plan itself. We'll discuss typical topics and components of a successful Disaster Recovery Plan in the following section.

The Policy Statement

The first heading in any type of disaster recovery plan should be a Policy Statement. A Policy Statement is a very broad-based statement of all the reasons your organization (or department) has for conducting the disaster recovery planning effort. Because this is a high-level statement, we often recommend that this be written by a chief information officer, or a chief executive officer; someone reporting directly to shareholders, the board of directors, or others with a financial interest in the company. Topics for the Policy Statement should include items such as "Protection of life."

It is difficult to help a company recover, obviously, if your employees are injured or killed. Because most of us are not philosophers or military people, I think it's safe to assume that human life would be the overriding concern in any disaster recovery plan. For both ethical and financial reasons, human life takes top priority in the process.

The Policy Statement should also contain references to minimizing the risk to the organization. Automated systems are put in place to help accomplish the company's business. These systems should not increase the risk to the company in the conduct of its business for the sake of convenience. The Policy Statement should say this, and also roughly identify the core operations of the business, or the items most crucial to keep running in the event of a disaster. References should also be included that speak to the issue of potential litigation or lawsuits in the form of shareholder suits or government-instigated actions.

Competitive Position is also a good thing to cover in the Policy Statement. A company that can't service its customers due to a failure of an automated system

will undoubtedly have competitors eagerly stepping in to fill that void and take that company's customers away. That's bad.

This leads to another topic for the Policy Statement, namely, Preserving Customer Confidence and Goodwill. Earlier in the book, the authors discussed a preliminary business impact analysis (BIA) and how to codify the financial impact of the disaster in terms understandable to an executive. An overview of this impact analysis may well be in order. Again, there won't be a lot of room for detail for such attention-grabbing statements as "the Company would lose one and a half million dollars a day in the event of a total equipment room failure," for example.

Finally, within the Policy Statement should be some kind of a synopsis of the recovery strategy, such as "We will restore any mission-critical automated system within eight hours."

These are all items that should be included in a good Policy Statement. Any reader of the Recovery Plan should be able to pick it up and very quickly determine the intent of having the plan.

Now comes the fun part. All of the items discussed earlier should be contained in no more than one page. Again, for this reason, this section should be very thoughtfully and concisely written, probably by an executive or someone ghostwriting for the executive, because these are very broad-based and corporatewide issues in scope.

To summarize the Policy Statement, it should contain statements that speak to the issue of Protecting Life, Minimizing Risk to the Company, Recovering Critical Applications, Safeguarding against Litigation and Shareholder Suits, Protecting Competitive Position, and Preserving Customer Confidence. It gives a very preliminary glimpse of the effect on business, in the form of a BIA summary and synopsis of the recovery strategy.

With all this said, let's get to the meat of the plan now.

Recovery Scenarios — The Three "R's"

There are several different ways to divide a recovery plan into a document that can be easily followed in a disaster. For the purposes of our example, I've divided this into what I'll term the Three R's: Reaction, Recovery, and Resumption.

Reaction — The First "R"

A disaster report may come into any one of numerous organizations within the company. A telecommunications disaster, because of water, for example, may first be reported to building facilities people; or it may be discovered by a security guard. The extent of the damage may affect not only the room but also multiplex equipment, servers, PBX, automated call distributing units, or other equipment. It may

not be immediately apparent, for example, to security personnel, whom to notify in the event that something wrong is discovered.

Similarly, if security persons were to find a broken lock in an equipment room, for example, they might be hard-pressed to decide for themselves whether anything is missing or damaged. It is possible, however, to codify some basic procedures for use in these situations, which should be global enough in nature to apply to any type of technical service department disaster.

One such precaution would, of course, be the protection of human life. A procedure could be written to secure the affected area, for example, and take any immediate precautions required to protect human life, such as evacuating the building, disconnecting power, or taking other emergency actions.

Similarly, police, fire, and emergency medical people should be immediately notified if required without taking time to activate a recovery plan. This could be done directly. It's better to err on the side of caution when lives are at stake. A procedure should also be in place to notify management and escalate the problem when anything unusual happens within the building. Because building-related disasters are often discovered first by the facilities or security departments, there should be a procedure in place in these departments' recovery plans to escalate these situations to responsible management and disseminate the information to responsible people throughout the corporation.

One flow, for example, may be from a building security guard to a building security manager, to a director of Technical Services, to a Disaster Recovery Response Team, to the appropriate departmental managers. The department response teams or disaster recovery managers, would then make a determination of the cause, if possible, try and evaluate the extent of the damage, and file an Initial Damage Assessment Report to either their management or to an Emergency Management Team (EMT).

The EMT

Let's talk for a moment about an Executive Management Team. The EMT is typically a core group of executives responsible for coordinating disaster response for the company as a whole. These are often chief technical officers, but not always. An EMT is called together only for the most severe disasters, which are corporatewide in scope. Typically comprising a half dozen individuals, these may include a Chief Information Officer, President of the company, the Director of MIS, the Director of Distributed Processing, the Director of Telecommunications, the Director of Facilities, and other high-level individuals. The EMT should also include one or two individuals to handle manning phones and routine administrative tasks, as well as coordinating supplies, materials, and other support required by the EMT. It's also very important that the EMT have a forwarding address, or a predesignated meeting place, a safe distance from the main place of business. This meeting place

could be an alternate company location, an executive suite, an employee's home, or even the Holiday Inn on the corner, for that matter. However, it's important that it be accessible at any hour and be known to the EMT and recovery planners well in advance. It should also be a place where telecommunications and telephone services could be prepositioned or moved in quickly after a disaster, to aid in command and control. A fax machine and e-mail should also be available in this alternate facility. Telephone numbers to the EMT should be prearranged with the telephone company in advance and reserved so they can be remote call-forwarded in a disaster. Again, this allows the numbers to be prepublished, both in company telephone directories, and in the Recovery Plan, which greatly increases command and control after a disaster.

The Initial Report to the EMT

After the first people arrive on site at the damaged facility, there should be a procedure in place for them to file an initial damage report to the EMT, usually within 90 minutes, to allow the EMT to make command decisions associated with the disaster. If the damage is sufficient to warrant such action, the EMT will then activate the remaining disaster recovery teams and a corporatewide plan.

The Telecommunications Department will be a key player in this plan, which will also be expected to work in harmony with other Technical Support and Facilities departments. For this reason, the Telecommunications Recovery Plan will have to comprise detailed responses to a variety of telecommunications-related scenarios. The plan should also have some information about the big picture, or where the Corporate Telecommunications Department fits into a companywide recovery planning effort.

The actual decision to declare a disaster or activate a computer, LAN, or Telecommunications Recovery Center should be made by the EMT after initial damage reports come in from the affected facility. The actual decision to relocate to a Recovery Center or an alternate processing location is also made by the EMT, again, after receiving the initial reports.

A large number of command decisions will have to be made in very rapid succession during the reaction phase of the disaster. For this reason, we also recommend opening a Critical Events Log, immediately upon being notified of a disaster. This is true both for EMT personnel as well as for Technical Service personnel and recovery teams. Everyone involved in a recovery effort will be working long hours and making many command decisions in rapid succession. This log is often no more complicated than a small, loose-leaf notebook that fits in a pocket or, for the more innovative, a voice tape recorder or PDA.

Every time an employee is called to make a command decision, it should be noted in the Critical Events Log. This could be helpful later on in analyzing the response to the disaster, and in dealing with insurance claims or litigation problems

that may arise. Many employees will rise far above and beyond the call of duty in responding to a disaster, and will need to be recognized afterward. These heroes should also be noted in the Critical Events Log.

Coordination with Local Authorities and Media

Coordination with local authorities is very important in the initial hours following a disaster. For example, if the building is out due to fire, many companies don't realize that the building does not belong to them anymore. It becomes a Fire Department matter, and the first order of business is for the Fire Department to take control of the building. Users will probably not be allowed to enter the building during this phase, and may not be allowed to enter the building, even after the fire is contained, because safety is a factor. This means any documents or magnetic media stored within the building will have to be assumed to be unavailable, which strengthens the case for storing these materials off site on a routine basis.

Disasters may also draw public attention, most notably television coverage or other media, which can be distressing to the business's customers, financial lenders, etc. The EMT will be expected to coordinate press releases through a well-organized corporate communications effort.

Once again, picture this scenario: The local television affiliates have just broadcast a statement that your organization has had a large fire. They have the mobile minicam on site interviewing employees of the company as they emerge from the building. The first two employees come out, smile briefly, and say, "Situation under control." The third employee, however, comes out screaming, "They're all dead in there! We'll never open again!" Which one do you suppose will be on television tonight?

If this is not the image you'd like to paint for your investors and customers, then a well-orchestrated media liaison is absolutely imperative in the plan.

Restricting the Site to Essential Personnel

Many employees have no business being on the site in the initial phases of a disaster, because (1) they can't do their job, and (2) they are not directly involved in the recovery efforts. Therefore, a policy should be in place to bar these employees from visiting the company, because it's also even possible that they could be apprehended or shot as looters. Even employees driving by the company describing the damage over their mobile phones to other people not involved in the effort could be tying up critical mobile phone frequencies, which could otherwise be used for the recovery effort. For this reason, the Recovery Plan should also contain a section that specifically forbids employees from using wireless phones in the vicinity of the company immediately following a disaster.

A designated individual should initiate the call to the EMT and provide the preliminary damage report to the EMT. These procedures should be outlined in the Departmental Recovery Plans. Similarly, individuals should be identified for making calls to clean-up companies, both for technical equipment or companies that specialize in hazardous spills or other specific areas of responsibility.

Persons responsible for coordinating with police, fire, EMT, and other local authorities should be identified in the Corporate Plan and delineated with a "Pointer" in the Technical Service or Plans. Technical service and telecommunications recovery plans ought to have a name and telephone number, as well as a "Pointer" to the Corporate Plan. The Corporate Plan should detail the responsibilities of this person or persons.

Accounting for Emergency Cash Disbursements

There are money-related issues that must be outlined in both the Corporate Recovery Plan and the Technical Service Recovery Plan. One would include a modified procedure for emergency signing authority for major equipment purchases. After a disaster, Technical Service Management, even midlevel management, may be called upon to replace high-dollar, expensive equipment very quickly. Therefore, procedures should be in the Recovery Plan both to modify signing authority, allowing midlevel management, under certain extraordinary conditions, to have high levels of statutory spending authority to accomplish replacement of equipment.

Other procedures should be in place to account for these expenditures, particularly when they're made in emergency situations and in very rapid succession. This will, of course, require close coordination with the Finance Department of the company, and the midlevel management tasked with making these purchases.

Other money-related items include, "Where would employees get cash in a disaster?" Very often, we have found plans in which technical employees who may be required to travel during a disaster, to disaster recovery centers or other locations, may not even have credit cards. They may also be unfamiliar with how to make travel arrangements, as the first time they are called upon to travel for the company may indeed involve travel to a Recovery Center to do their job.

One instance we've seen, which addresses this problem very effectively, is for the company to sign an agreement with its primary bank, which mandates that the bank will have a mobile "bank on wheels" on site within 2 hours of a disaster. This mobile bank should contain two bank employees (for obvious reasons, when there are large sums of cash changing hands,) and be responsible not only for the dissemination of cash after a disaster, but also for the accounting of it. If your company does a large amount of business with a bank, it should agree to this type of stipulation; otherwise, maybe you need a new bank.

Issues Involved in Moving People

For companies moving hundreds of employees, particularly nontechnical employees, to recovery centers, cash may be the least of their problems. There are many documented cases on record when nontechnical people had to move, in rapid succession, to recovery centers, to do their jobs. For starters, some don't go.

For another, think about what happens when the order is given for them to relocate. Many employees have never been on a plane. Think of all the excuses you could be given, immediately following a disaster declaration, and all the people-related problems. "I have children." "I'm on prescription medicine." "I don't have a credit card." "I don't have any money." "Who will take care of my sick mother, father, sister, and brother?" "Which airline should I take?" "Where should I stay?" "Where should I eat?" "How do you rent a car with no credit card?" It becomes obvious, very quickly, that these procedures also must be identified in the Recovery Plan.

A travel agent should be predesignated in advance and have emergency instructions for your company on file. Then, employees could call the travel agent on a 1-800 number or whatever, and have decisions made for them on a predetermined itinerary. Once again, the importance of preplanning and getting procedures in place cannot be understated.

Maintaining Security during the "R"eaction Stage

Other parts of the initial reaction phase include items such as maintaining security at the damage site. After a major disaster such as a tornado or fire, a lot of people will be on site. Which of these people are employees, and which of them are looters? (I've often been told by my people that without my business attire, when I'm off work, I usually look like a looter. I would certainly appreciate having something in the Recovery Plan to identify me so I'm not shot!)

Issuing all employees authorized to be on site after a disaster, an identification badge, hard hat, flashlight, and an orange vest can alleviate this problem. The identification badge is to immediately identify the person as an authorized on-site employee, a hard hat and flashlight, for obvious reasons, as people would be expected to return or come into the building after the disaster, and the orange vest is for visibility. It is important to think ahead and identify your employees before they show up on site.

Other security-related concerns could include looting of the building. If recovery is taking place at the damaged site, a lot of equipment will be moving in and out in rapid succession. There will be several trucks on scene, and it will be very easy for theft to occur. It is also important to identify the persons responsible for security on site.

Security should also be of concern at the mobile funds disbursement center that was described earlier. An off-duty police officer or two is a good idea at these centers.

The "R"ecovery and "R"esumption Phases

After the initial reaction to a disaster, we get down to the long business of recovery and business resumption from the disaster. Most of the Recovery Plan will be concerned with these issues.

A large number of the restoration activities involved in recovering from the disaster will have to be coordinated between various technical departments. Whereas each individual technical department, such as Telecommunications Managers, LAN managers, and Mainframe Managers, will coordinate the restoration of their respective hardware and software systems, other systems that are common to the site will have to be coordinated for restoration. These include such systems as power and wiring systems.

Everyone has an interest in electrical power, and everyone has his own specifications for it. Mainframe managers will have special power requirements, such as 400-cycle power for computer equipment, whereas Telecommunications managers may need elaborate batteries and 48-V systems. Of course, building power will be required by everyone.

One particular technical service department will either have to take the lead on the issue of power, or the Facilities department will have to take the lead, with intensive coordination of all of the various technical service departments to ensure that proper power is provided.

Other seemingly small problems can become major issues in the recovery process. These include oddball plugs for power, which may not match the receptacles on the new equipment. Other common systems, such as fire suppression systems, sprinkler systems, Halon, and the like, may have to be coordinated by the building facilities people as well.

Rewiring the Facility

Rewiring of the facility, however, is where the fun really starts. In today's equipment installation, all types of wiring is run throughout the building. It is important to document the various types of wiring required for LANs, telephones, and other purposes throughout the facility. A detailed wiring diagram and schematic should be maintained within the Recovery Plan, detailing various levels of cable required for LANs, telecommunications, and a rough layout of the physical path in which the cable is run. It will be difficult during the restoration process to have various contractors, each for the Telecommunications, LAN, and other departments, all

trying to work at the same time, in the same crawl spaces and conduits. Therefore, close coordination of the departments and the contractor should be the rule.

Testing the New Hardware and Software

Other issues will also surface during the restoration process. These include, for example, testing new hardware that is installed. It would be imprudent to risk a double-dip disaster by not adequately testing newly installed hardware and software before going back to the primary location. Therefore, procedures and checklists for testing this hardware after it is installed are imperative. Similarly, operations personnel may have to be trained on the newly installed software and hardware, the recently installed equipment may have changed with time, or it may be different equipment altogether from what was originally installed.

On a related issue, the actual employees utilizing the equipment will also have to be trained. For example, picture what it would be like to have a customer service center of perhaps 100 employees, and newly installed equipment. If these employees had previously been on Windows 2000 personal computers, for example, they would probably not be restored on Windows 2000 after the disaster. Management might instead purchase software that is more up to date. The same holds true for the hardware. It could prove to be a very daunting task indeed if 100 employees all converged on the technologist, saying, "Gee! The function key used to be here, but now, it's over here!" or, "The screen used to paint this way, but now it paints that way!" or, "I used to get a window here, but now I don't get one at all!"

Training issues can greatly exacerbate restoration from a disaster, particularly in an already confused environment.

Returning to the Damaged Site

Finally, scheduling a migration back to the original site if a Recovery Center is used, or coordinating a return to this site, could also be a touchy situation. As we already stated, one must not risk having a double-dip disaster by moving too quickly. Yet, recovery centers are expensive, and they do encourage users to get out as soon as possible. Because most recovery centers usually want you out in six weeks or less, the user must move somewhere. The situation might indeed be one of "Ready or not, here we go!"

Also, realize that, for some period of time, the company will be running two data centers while the conversion back to the original site is being accomplished. During this time, it could be difficult to operate with the existing staff spread thin between the two locations.

People Concerns — Burned-Out Heroes

One final concern during this restoration process is your people, themselves. In any major calamity, we have heroes, and we have turncoats. Let me explain.

One can almost chart human motivation in response to a disaster, much like Figure 6.4. In the beginning, you'll note that motivation or productivity, or whatever word you care to use, takes a distinct drop. This is around the time when people are initially notified of the disaster and say to themselves, "Gee, I guess I'm out of a job," and tend to feel very badly about what happened. Afterward though, or at some point, it becomes apparent to the employee that he or she might be able to pull this out of the fire.

At this point, something very phenomenal happens, and productivity skyrockets. This is because most people work well in the hero mode. People work almost superhuman hours, sometimes 16 or 18 hours a day, sleep on the job, and do everything possible to pull the company out.

One amusing story I once heard was about a company with an employee, as it turns out, a key programmer, who would work like crazy as long as people kept him supplied with Twinkies and Cokes. As part of this company's recovery plan, there was a line item that indicated, "Where to get Twinkies and Cokes" for this person should a disaster occur. Most people are working for even more than Twinkies and Cokes, however; in a major disaster, they could be working for their livelihood. It's hard to find work these days. Therefore, they exhibit an almost superhuman effort to help the company recover, working long hours, and productivity takes off. Near the top of this curve, something happens. At this point, exhausted employees optimistically announce to each other, "Gee, I think we're going to make it!" At that point, something equally predictable happens; productivity begins to fall, almost as drastically. Often, the average employee now is working on a folding table with wires run everywhere in a makeshift setup. It's easy now for different thoughts to come to mind. Rather than thinking like a hero, the employee begins to think,

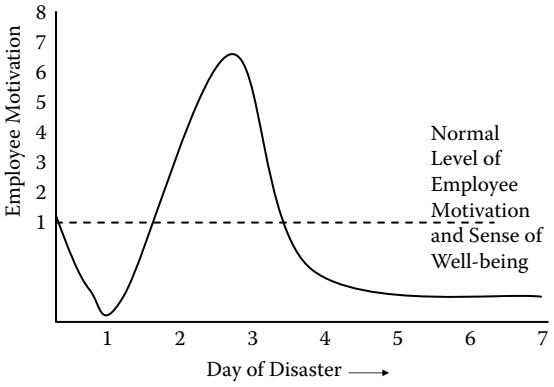


Figure 6.4 Variation of employee motivation with time.

"Gee, it really stinks working down here in a basement!", "Gee, I really hate working on a folding table, I wish I had my office back.", or "This person next to me yaps on the phone all day! I can't get any work done. I wish he would shut up!"

Something else begins to happen at this time. These employees may begin to get calls from recruiters, saying, "Hey, I have a nice, roomy, corner office on the 17th floor! Why don't you come to work for us?" And that's exactly what happens sometimes. Either through burnout or being fed up, or for whatever cause, these employees begin to jump ship. This could be a terrible problem for a company just beginning to get its bearings again after a major disaster, especially if they are key people who defect. By this stage of the process, even Twinkies and Cokes may not be enough.

Another very predictable issue concerning your people involves how they react upon an initial disaster notification. There are many documented cases, for example, of hurricanes, where employees receive notice of a pending hurricane coming in, and are put on alert for a companywide disaster. Almost without fail, the employees would first go home, board up their windows, and ensure the safety of their families before reporting back to work. Case in point: this scenario became commonplace during the 2005 hurricane season. Unfortunately, by the time the employees were ready to return to work, many of the bridges were already under water or the roads were otherwise impassable because of the storm. In these cases, recovery activities could not commence until the "all clear" was given and the situation had eased.

Similar dynamics occur in the case of major earthquakes and other disasters. If your company is situated in an earthquake zone, your plan must take into account that the employee's first concern will be for their families, and you may have to expect a delay or the loss of key people returning before you can commence your recovery efforts. Indeed, maybe members of the EMT itself will not show up at the company until they are satisfied that their family is safe. This is just a normal, human tendency. There is nothing that can be done about it but it should be taken into account.

Some companies have experimented from time to time with making provisions for employees' families. For example, if your building is a hardened facility with extra room, you may, in fact, want to make provisions for employees' families to stay there in the building in the event of a widespread disaster. I realize the lawyers will have a fit over the liability issue. In terms of peace of mind, however, if the employee is satisfied that his family is safe, the employee will be better able to concentrate on the business of helping the company recover. This outweighs, in my opinion, the liability. Besides, that's why there's insurance.

This is probably not unlike the situation that occurs on many military bases during alerts and storms, when dependents are called into on-base facilities to stay until the situation blows over. Anyone who served as I did will remember. Maybe that's why I like the idea.

To summarize, be mindful of the feelings of your people in a disaster as well because recovery without them is impossible.

Other Scenarios

Depending on other factors, such as geography, the Recovery Plan may contain specific responses to various types of disasters. For example, there may be specific procedures on what to do during an earthquake. Many companies in the Midwest have some type of a tornado drill in the Recovery Plan. Those on the Gulf Coast, well, you know …

There should be some type of a generic procedure in the Recovery Plan regarding what to do if an employee discovers sabotage or vandalism within the organization, to either technical equipment or other property. Most companies today have documented bomb threat procedures. For example, operators are drilled to listen carefully to anyone calling in a bomb threat. Are they laughing? What tone of voice is it? Are they male or female? What age do they sound? Are there background noises that might give away their location? These should also be dovetailed into the Recovery Plan for easy access should the occasion arise.

Procedures for power loss or power failures might also be written into corporatewide standards somewhere and should also be written into the plan, or at least referenced in it.

What if you found yourself in this scenario? Let's say your company has just fired an individual. However, rather than just firing the individual, you watched this individual as he was dragged by two security guards to the front door, screaming, "I'll get you for this!" Now, today while you're home, enjoying the day off, you get a phone call. They say they "just saw this person inside the building, and they don't know where he is!" How badly would you feel about that? It could happen. It has happened.

I had occasion a few years ago to tour an underground data center, completely redundant, with water evacuation systems, state-of-the-art fire protection, even a cipher-lock system that weighed people before letting them into the facility. The site was 6 ft below ground. Upon remarking what impressive security the site had, the site manager remarked and in a calm voice said, "Yes sir, we're protected against every unforeseen event, except an employee who gets pissed off at us!" In light of these facts, procedures on what to do in the event of any kind of a security breach at the organization should absolutely be a part of the plan. An employee with a bomb or other device could be destructive, but an employee in a data center with a permanent magnet, could be even worse.

Finally, if the company has any procedures for heavy snow, tornado watches, or other weather-related disruptions, these should be referenced and pointers should be included in the Recovery Plan as well. The corporate Telecommunications Department, for example, may even provide a 1-800 number, 1-800-DISASTER, for example, where employees could call in and not only learn about the status of systems during normal operation but also get special bulletins regarding weather or corporate disasters during times of emergency.

Summary

To summarize, the Recovery Plan should begin with a thoughtfully written Policy Statement, outlining all of the objectives of the project and the overriding theme. The primary interest should be protection of human life, with other concerns, such as minimizing risk to the company, and preserving customer goodwill as secondary considerations. It is also helpful to think of the recovery process in three terms, or the Three R(s): Reaction, Recovery, and Resumption. Regardless of which technical service department you're in, the Recovery Plan for your given technical area should contain a series of pointers to establish policies in the corporate Disaster Recovery Plan and to ensure continuity throughout the organization. These ensure that items which are global, or companywide in nature, such as who notifies police, fire, and medical, or who talks to the media, are defined, and that these activities proceed flawlessly.

We spoke about the concept of an EMT (Executive Management Team), which serves as a focal point for coordinating recovery activities. It is the EMT that actually makes the decision to declare a corporatewide disaster. We talked about using caution when interfacing with customers, financial lenders, and the media, and carefully controlling these activities through an established, corporate communications process. We spoke of the damage assessment phase of the recovery process, notably, who activates the EMT, when to activate the EMT, and how to notify the EMT, as well as providing timely reports to the EMT for adequate command and control and making sound decisions regarding recovery of the company.

Remember to consider items such as opening a Critical Events Log for audit purposes, and don't overlook financial concerns, such as signing authority for equipment purchases, or where your employees can expect to get cash. Don't subject your area to possible looting by neglecting security at the damage site; don't risk a double-dip disaster by not adequately testing the newly installed hardware or software systems, or by relocating from your recovery site back to your regular site prematurely, before these systems are ready. Don't overlook training issues, for both your Operations people as well as employees; and lastly, be ever mindful of the concerns and the sensibilities of your employees, particularly with regard to the welfare of their families in widespread disaster situations. Realize that when earthquakes or hurricanes occur, employees may not be available immediately for a prompt recovery.

Finally, remember the productivity curve that we described earlier. Realize that although employees may work in a superhuman fashion during the recovery process, most cannot keep up this pace for weeks on end. Some will leave the company, whereas others will crack up. Therefore, after the recovery process is complete, it is highly recommended that the company sponsor some type of forum to recognize the heroes and to schedule some very well-needed compensatory time off.

This section has talked much about the generic issues of disaster recovery and introduced the concepts of pointers, and how the technical service and

telecommunications Recovery Plan needs to dovetail into the overall corporate Recovery Plan.

In the next section, we will get into the actual details of a Telecommunications Recovery Plan, including some examples of failures in telecommunications systems, and how the company should respond to these. We will also cover the final "R" — Recovery — in detail relevant to the technologist. Although this section has been very generic in nature, the next one will be very specific, concentrating on a very focused area of disasters in technical or computer platforms. We will also draw many parallels between the Disaster Recovery Plan and the Operating and Security Standards document discussed in the past chapters. Because so much of telecommunications recovery planning is proactive rather than reactive in nature, it becomes very important to have a strong set of operating and security standards for the day-to-day telecommunications operation, either as an integral part of the Recovery Plan, or as a stand-alone document, which is frequently referenced inside the Recovery Plan.

A successful Disaster Recovery Plan depends to a large extent on the strength of the standards applied to the day-to-day operation of the mission-critical systems that support the core operations of the company. In some cases, prevention is the only defense a company has against the telecommunications disaster, because, after the fact, often, little can be done.

The following detailed section will combine a set of restoration procedures with these operating and security standards that in sum total will be the Disaster Recovery Plan protecting these systems for the company.

CHAPTER 6
WORKSHEETS

DOCUMENTING THE PLAN!

WORKSHEET No. 1

Equipment Inventory

Equipment _____

Manufacturer _____

Serial # _____

Software version _____

Criticality rating (5 = most critical 4 3 2 1 = least)

Date of purchase _____

Remarks

_____

_____

_____

_____

_____

WORKSHEET No. 2

A Great Equipment Inventory

Have you visited the Finance Department to discuss their object-linking into your Recovery Plan? Here is how:

- Any time equipment is purchased, the approval forms (including what was purchased) go to Finance, right?
- Have Finance scan these forms into a file called equipment-inventory.doc. If they are electronic, save them to this file.
- Object-link equipment-inventory.doc into your plan.
- Update your standards documents so that this procedure always gets done.

Here are more details:

WORKSHEET No. 3

Software Inventory

Software _____

Manufacturer _____

Serial # _____

Software version _____

Criticality rating (5 = most critical 4 3 2 1 = least)

Date of purchase _____

Remarks

_____

_____

_____

_____

_____

WORKSHEET No. 4

A Great Software Inventory

Have you visited the Finance Department to discuss their object-linking into your Recovery Plan? Here is how:

- Any time software is purchased, the approval forms (including what was purchased) go to Finance, right?
- Have Finance scan these forms into a file called software-inventory.doc. If they are electronic, save them to this file.
- Object-link software-inventory.doc into your plan.
- Update your standards documents so this procedure always gets done.

Here are more details:

WORKSHEET No. 5

Employee Callout List

WORKSHEET No. 6

Building Facilities under Floor Grid Diagrams

WORKSHEET No. 7

Putting Something to Paper Now

Cut and paste from Chapter 6 into the fields on the following pages, with your own modifications. Use other good sources too and don't forget to import data from established company procedures and known good sources!

WORKSHEET No. 8

I. Mission Statement

Write a compelling Mission Statement here, with the input of senior management. It should be no more than a paragraph long, including concepts such as protection of life, recovery of operations, protections of shareholder well-being, etc. Refer to Chapter 6 for more information.

Mission Statement

WORKSHEET No. 9

II. Overview of the Recovery Plan

Notification of Police, Fire, EMT

Notification of Management

Determining the Cause

Filing Damage Reports

Security at Affected Facility

Names of Recovery Teams

Activation of Recovery Teams

Decision to Declare Disaster — How

Decision to Activate Recovery Center — Who

Relocation to Recovery Center — Where

Coordination with Local Authorities — When

Notification of Customers, Lenders, Media — Why

Activation and Coordination of EMT

Notification of Clean-Up Companies

When to Open a Critical Events Log

How to Get Cash

WORKSHEET No. 10

III. Companywide or Interdepartmental Disasters

Fire

Flood

Earthquake

Tornado

Sabotage/Vandalism/Theft

Bomb Threat/Security Breach

Power Failure

Bird Flu Outbreak or Other Pandemic

Contamination

Medical Emergency

WORKSHEET No. 11

IV. Telecommunications Disaster

Consult Chapter 6 or 7 on these issues.

PBX, ACD, or Voice Mail Failure

Cable Cut/Fiber Cut

Failure of Major T1 Node

Failure of Router, Switch, or Front-End Processor

Loss of AT&T Central Office

Loss of Long-Distance or 800 Carrier

WORKSHEET No. 12

V. Appendices to the Plan

Import all of these that you can by object-linking your plan to established corporate policies or known good sources. Designate the file name here in advance, as follows:

Appendix Number/Title	*Department Where File Is*	*File Name to Import to Plan*
Recovery teams	Human Resources	Teams.doc
Escalation lists	Network Control/help desk	Escalation.doc
Inventory forms	Finance	Inventory.doc
Carrier lists	Network/Telecom	Carrier.doc
Maintenance forms	Internal Audit	Maintenance.doc
Hardware lists	Finance	Hardware.doc
Software lists	Finance	Software.doc
Team duties and responsibilities	Executive	Duties.doc
Network diagrams	Network	Network.doc
Floor diagrams	Facilities	Floorgrid.doc
Contract and maintenance agreements	Finance/Legal	Contract.doc
Special instructions	Various	Special-telecom.doc Special-MIS.doc Special-LAN.doc Special-Power.doc
Wireless phone inventory	Purchasing/AP	Wireless-phone.doc
All other		

WORKSHEET No. 13

Now Try Your Own

1.	Recovery teams Write or insert (object-link) teams.doc
2.	Escalation lists Write or insert (object-link) escalation.doc
3.	Inventory forms Write or insert (object-link) inventory.doc
4.	Carrier lists Write or insert (object-link) carrier.doc
5.	Maintenance forms Write or insert (object-link) maintenance.doc
6.	Hardware lists Write or insert (object-link) hardware.doc
7.	Software lists Write or insert (object-link) software.doc

8.	Team duties and responsibilities Write or insert (object-link) duties.doc
9.	Network diagrams Write or insert (object-link) network.doc
10.	Floor diagrams Write or insert (object-link) floorgrid.doc
11.	Contract and maintenance agreements Write or insert (object-link) contract.doc
12.	Special instructions Write or insert (object-link) special-telecom.doc special-mis.doc special-lan.doc special-power.doc
13.	Wireless phone inventory Write or insert (object-link) wireless-phone.doc
14.	All other Write or insert (object-link)

Chapter 7

Writing a Telecommunications Recovery Plan

Leo A. Wrobel

Contents

Telecommunications: Specific Recovery Procedures 181
Telecommunications' Role in Seamless Solutions 184
Other Telecommunications Recovery Concerns 190
Physical Vulnerability to Telco Disasters — Where Does One Start? 200
Callout of the Telecom Recovery Team 210
Software Disasters..... 212
Major Cable or Fiber Cut..... 213
Risks with T1 Service Utilizing Proprietary Multiplexers or Routers..... 214
Forms Associated with the Plan 216
Other Tips..... 219
Summary..... 219
Recovering Emerging Technologies (Frame Relay, VoIP, ATM and More)..... 221
Chapter 7 Worksheets..... 233

Telecommunications: Specific Recovery Procedures

To completely understand the subtleties of recovery planning for telecommunications-dependent businesses, it is important to understand the new modes

of operation inherent within these enterprises. We will begin by describing the way these businesses operate today, and how they are profitable and make money without ever seeing a customer coming in the front door. This ability is highly dependent on a strong integration of both telecommunications and data processing capabilities, often referred to as a "seamless solution."

Let's start by revisiting a diagram that is a variation of the "seamless solution" mentioned earlier in this book. This represents a hypothetical manufacturing company that has become deeply dependent both on open systems and telecommunications technology. Let's trace the path of a typical order through the company and explore how immediate access to information strengthens the process across the board and makes the company more profitable.

The first thing you'll note is that the process, like any good process, begins and ends with the customer (Figure 7.1). Starting on the left-hand side of the figure, you see a customer dialing in, probably on an incoming 800 number, to a customer service center. This customer service center will utilize many types of integrated technology to handle the load. These would include ACDs (Automated Call Distribution Units), a connection to some type of data processing capability, probably a LAN someplace to put people where they can sit and answer calls, and lastly, local and long-distance service. Integrated technology turns the whole thing into a revenue generator because, again, this business has no storefront.

In this hypothetical manufacturing facility, the Customer Service Center answers a call inquiring about a product. Let's assume it's a certain type of integrated circuit chip. The customer calling in may be someone who works for Ford or General Motors, inquiring as to whether the chip is suitable for a particular automotive application. In such a case, it may not be readily apparent to the Customer Service Representative whether the manufacturer's products are suitable to the caller's application. Perhaps it represents a new market for the company. Therefore, rather than telling the customer, "Leave your name and number with me, and I'll call you when I get the answer," the Customer Service Center

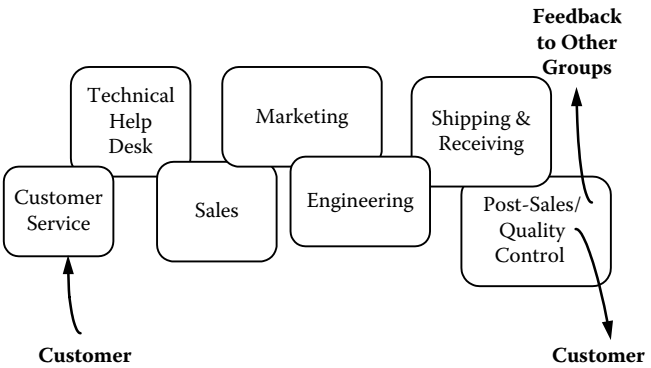


Figure 7.1 Seamless solution.

employee can respond in a very different manner by virtue of his or her access to data. The Agent might make an inquiry online to Sales, for example, to find out if similar sales for these types of automotive applications have been made in recent time. Sales or Customer Service, in turn, can make an inquiry to Systems in the Engineering Department, illustrated by the third circle, as to whether it's feasible to adapt an existing product. Customer Service, Sales, and Engineering may make an inquiry to the Production people to learn how long it might take, for example, to adapt to this product.

Access to this information means one thing: the Customer Service Center can respond quickly, efficiently, and accurately to a customer's inquiry while the customer is on the phone and hot to buy. What might have been a "I'll call you later," now becomes, "Yes, we can adapt an existing chip to your application. Engineering says it will take a week; we can produce it within two weeks. How many would you like to order?"

It's possible, by looking at Figure 7.1 to trace the path of a typical application and think to oneself how the entire process is strengthened by virtue of the fact that many disparate organizations in the company have access to each other's information.

The last rectangle labeled Post-Sales would be a function used later. This department would call the customer and ask questions such as, "How was the product?" "Did it meet your application?" "Would you like to place another order?" "Are you aware that we offer other products that may fit an automotive application?" "May we send you information on these products?" This feedback in turn is filtered back to the Customer Service Center to strengthen that operation for the next call.

The seamless integration of all of these various disparate operations into one synergistic entity is probably the single most important reason for migrating to a client/server architecture. The access from potential customers either via the Web or over a 1-800 number is what switches these amazing capabilities on.

But what happens when telecommunications links fail? Although the local network can be backed up for short periods by perhaps falling back to manual paper processes, if customers can't call you at all, that's worse.

With these thoughts in mind, let's look at the diagram from a disaster recovery perspective. Which circle would you say is most important in the process as far as the company's long-term profitability? Most would answer, "The Customer Service function," and this answer is probably correct because the walk-in market for customized computer chips, as shown in this example, is probably small. Most of this company's business would come over the phone first and then be totally dependent on automated systems. Therefore, as technologists, our job becomes one of looking at what technical platforms support the Customer Service Center in making these as fault-tolerant and resilient as possible. Part of this process will be selecting equipment with a very low failure rate for use within the organization. Another equally important part, however, will be selecting telecommunications providers capable of rising to the call. Even the most sophisticated

and fault-tolerant network topology can be quickly rendered useless in the event customers are incapable of calling you. Therefore, we'll concentrate in great detail on evaluating a telecommunications provider for fault tolerance and resiliency later in this section.

Bringing Business Closer to the Customer

Earlier in this book we used companies such as 1-800-FLOWERS and Home Shopping Club as shining examples of how companies become very successful simply by making it easier for users to avail themselves of their services. Consider 1-800-FLOWERS; this is their telephone number: 1-800-F-L-O-W-E-R-S. Now, forget the number! Get the picture? By making it easy for a customer to avail themselves of their service, namely floral delivery, the company has become a resounding success. At the same time, however, look at the amount of their business that is dependent upon telecommunications. It's virtually 100%.

Think about the second example, Home Shopping Club. Companies like this one depend upon very fast turnover of products to be profitable. The products advertised on Home Shopping Club may only reside in the warehouse a few days because the money is in turning them over and selling them to consumers, not in storing them. These are advertised on television, and the consumer is given an 1-800 number to call to order for UPS delivery. Once again, consider the dependence on telecommunications! A single cable cut by a wayward contractor, for example, could isolate a company like this one for several hours or days, resulting in virtually a 100 percent revenue interruption because all the business, again, comes over the phone.

Telecommunications' Role in Seamless Solutions

A number of years ago, while visiting a client in Dallas, I telephoned a busy travel agent in New York. Upon ringing in, I learned that the travel agent was not doing any business all day because of a major cable cut on the AT&T network. In fact, they were surprised that the phone rang at all because, as an AT&T user, they were getting very few calls. The client that I was visiting happened to be an MCI customer, which meant that, in this particular case, they were not affected by the outage. Now, before people begin thinking that I'm making fun of AT&T, let me make a couple of points.

First, any and all long-distance carriers have periodic troubles. This is not an MCI commercial, but on this particular day, it just happened to be AT&T's turn in the barrel. Similar events have happened to MCI in which AT&T customers remained untouched. The point that I'm making here is that a busy travel agent was down all day due to a long-distance company failure, and, as pointed out earlier, a

good percentage of their business came over the phone. Today, the walk-in market for plane tickets is very small.

The fact, however, that one long-distance company was in trouble whereas the other was untouched should illustrate that some preplanning may have avoided this outage. If the travel agent, for example, had diversified its incoming service over several carriers, the chances of being isolated during a major failure would have been lessened. We'll talk about this somewhat in this section, as well.

One other thing that's probably important to note, very much to AT&T's credit, is a series of new service guarantees for incoming 800 service and private line service. Today, AT&T and other carriers guarantee that an interruption in 800 service could be redirected to another working number in less than ten minutes. Similar guarantees are developing for private line service, most notably services like FASTAR or NRS. Sprint built its network into a series of fault-tolerant fiber-optic loops in the 1980s and 1990s, which provide a measure of protection as well. This was later adopted by most of the major carriers. Other carriers still diversify by using microwave radio, for example, to back up fiber-optic groups that may be prone to an accidental cut. After all, it's still hard to dig up air. All of these measures show a new sensitivity by carriers to the importance of telecommunications and its role in the core business operations of its customers. By mixing both telecommunications carriers and services in an optimal configuration, a high level of network reliability and availability can be achieved. Combined with the I/P or ATM protocols (packet or cell based rather than TOM switch based), the network has become even more reliable. Stated in lay terms, if a fiber ring gets cut, packets and cells can find another route another way around. The same holds true with other technologies such as frame relay. Therefore, although dependence on telecommunications is much greater, the technologies available to back it up are more numerous today.

The Business Recovery Concept

Over the years, there have been many areas of focus for disaster recovery planning depending on the dominant competing technology of the times. In the mid-1960s, companies became dependent on mainframe computers, which resided in "hardened" computer installations. The name of the game, in these cases, was to take all of the preventative precautions possible to ensure that a disaster never hit this critical nerve center. This included everything from Halon fire protection to no-smoking policies and to water detectors under the floor. These were discussed earlier in this book. By the early 1980s, telecommunications gained prominence, particularly when the price of these services dropped after the 1984 AT&T divestiture. In the mid-1990s, client server began to take on a prominent role to deliver more rich applications to the desktop. With every change, auditors and technologists fretted

over the migration of mission-critical applications from the comfortable mainframe platforms to the more unproven and telecom-dependent client/server platforms.

Today, client/server has evolved to a reliable platform and, in some cases, even rivaling mainframes in terms of availability and support. The issue of disaster recovery planning, however, has not gone away. In fact, it has broadened. By successfully applying these technologies towards core business applications, as described earlier in this section, companies have become much more profitable and efficient. At the same time, new areas of vulnerability have opened, principally in areas of telecommunications. It becomes very apparent, early on, that all the services required to complete a sales transaction must be restored for the recovery solution to have any value. These include:

1. An attendant position (a place to put people).
2. Connection to some type of automated data processing facility (e.g., LAN, mainframe, or both).
3. Telecommunications capability for voice and data.

A combination of these three components comprises a business recovery solution. Without any one of these three components, the company's core business and revenue-earning capability grinds to an abrupt and costly halt.

Because this is the telecommunications section, we will concentrate mostly on the critical telecommunications link, which turns the people and the automated platforms of the company into revenue generators.

Incoming 800 Service

A considerable amount of marketing effort has been expended by the carriers advertising service guarantees for 800 service. This is probably money well spent because even senior executives who are nontechnical understand the importance of being able to answer incoming calls. The most dynamic and compelling commercials broadcast are likely the ones that show telemarketing centers; for example, full of people sitting there knitting, filing their nails, and doing everything except answering the phones. The implied message is, "How long can your business survive a disruption like this?"

In reality, switched telephone services of all types, including 800 service, are some of the simplest components to backup, that is if you preplan in advance. We spoke earlier of service guarantees offered by AT&T and all other carriers that guarantee the redirection of any 800 number to any working 10-digit telephone number in North America within 10 minutes. This would allow your organization to direct calls to another company location, or perhaps, in extreme cases, even allow employees to answer these numbers at home. Other options include finding a hotel suite or a ballroom in a major hotel. In addition to space availability for

putting people back to work, hotels also have fast availability of telecommunications services in many cases because they have large PBXs.

Think about the possible locations for redirecting your critical 800 lines within your company, and then develop a form, or use Worksheet 1 at the end of this section to document them before a disaster happens.

Incoming Telephone Service

Like the 800 service, incoming telephone service can be quickly redirected in many cases. Rather than calling the long-distance company, the call is made to the local telephone company, such as Ameritech or Bell South. Once again, the physical capabilities of today's network allow for the redirection of critical incoming numbers to any working ten-digit number in a matter of minutes. Many local operating companies, in fact, even allow for the redirection of direct inward dial (DID) trunks under a special assembly basis.

Once again, this must be done in advance to allow for the most flawless recovery. A similar form can be developed, such as Worksheet 2, to document redirection of these critical numbers in advance, as well.

Private Line Service

Unlike the incoming 800 and incoming telephone services, private line circuits such as T1 and T3 can be difficult and complex to restore. Nonetheless, they provide access to databases and ordering systems, which are one of the "Big Three" outlined earlier. Remember that we need access to the data as well as the customer in order for the company to function. In cases of switched services, such as 800 lines and telephone service, a company could probably limp its way through, even without documentation, by depending on the telephone company. This, of course, also assumes that the disaster is limited to one company, and the telephone company is not busy elsewhere.

In the case of private line service, however, preplanning and pre-coordination is absolutely essential because these are customized, hard-wired data services that do not move easily. One common example might be a firm with a mainframe disaster recovery plan but no plan for a LAN or telecommunications. This could, in fact, be worse than no plan at all.

Consider what types of applications reside on a mainframe. These are usually categories like financial applications in payroll, which management has been too skittish to move to a client/server technology. These would, presumably, be in business at the recovery center.

Now consider which applications reside on the LAN. These are all the applications that make money for the company and directly support the sales and production process. The applications, in this case, would presumably be out of service.

Telecommunications is the other half of the equation that turns the LAN into a revenue generator; however, in this case, telecommunications would also be out of service. Thus, the company ends up in the unenviable position of being able to run payroll and accounts payable, and all of the other applications that channel money out of the company, while not being able to perform any of the applications that bring money into the company. I don't know about you, but I would rather not have a plan at all than to be in this position.

Therefore, if your network depends on private line service to provide access to the systems described earlier as the "Big Three," pre-planning will be absolutely essential. As a minimum, document the circuit number of all private line circuits, its intended use, and priority on a specially designed form (see Worksheet 3). After you've done this, get together with your local and long distance telephone companies and inquire about possible solutions for backing up these services. It will also be helpful to review the earlier parts of this book where backup and recovery options for private line service were covered in detail.

Day-to-Day Protection

It need not be a dramatic disaster to cost your organization money, particularly if you're an organization without a storefront that is operating with a modern, seamless architecture. One cable cut that isolates your network all day may be enough to deprive your company of 1/22 of a month's income if you are only open on weekdays. (There are 22 business days in a month.)

Because telephone cable cuts are such a common occurrence, let's briefly cover some of the ways we may protect against them. These are, once again, covered in great detail at the beginning of the book. For the purposes of this chapter, let's have a quick review.

Fiber-Optic Cable Cuts (Long Haul)

The example we discussed earlier about the busy travel agent out of service all day was due to a cable cut on a fiber-optic cable. When selecting a long distance carrier, it's important to evaluate the type of protection they provide against this possibility. Use Worksheet 4, this chapter, as a guide when making inquiries to a long-distance company about their contingency plans for a major fiber-optic cable cut.

Local Cable Cuts

Local telephone cables, commonly referred to as the "last mile," are also a constant source of disruption. Because these run through metropolitan areas where construction is frequent, it becomes very easy for construction crews to either dig up or

core through these cables. Use Worksheet 5 as a guideline on measuring the commitment of the local operating company to the avoidance of such disasters.

Software and Traffic Management Disruptions

Many times, disruptions to telecommunications systems, particularly switched telephone service, are due not to hardware failure but to software or traffic management failure. A few years ago, the city of Dallas, Texas, had a 4-hr-long disruption, where it was difficult to place any type of telephone call in the Dallas metropolitan exchange. This was due not to a cable cut, tornado, or hurricane, but to the fact that Garth Brooks concert tickets went on sale that day. Radio announcers broadcast this over the air, and the network was swamped with calls, making other types of telephone calls difficult or impossible. Similarly, software failures may also affect the network. Most modern central office (CO) switches have an elaborate series of software codes, blocks, and classes of service, which can be difficult to troubleshoot in the event of software failure. Remember, even in the most confident local operating companies, the personnel are still more comfortable with telephone test sets than with data scopes. Use Worksheet 6 to aid you in evaluating the potential for this type of problem.

Summary

Consider that telecommunications is part of an overall business recovery solution that encompasses what we referred to as the "Big Three." Recall that these three include:

1. Attendant positions
2. Connection to the data
3. The telecommunications services, which turn the three into revenue generators

Look carefully at your business and the core business services it is intended to offer. Scrutinize the technical platforms that support these core businesses and provide revenue to the company. Be mindful of the fact that you are probably the company's storefront, and without the automated systems you provide, revenue production for the company becomes impossible. Understand the role of seamless solutions in the long-term strategy of your company and don't be bashful about providing your technical input. By virtue of the technical systems you provide and the preventative steps you take to protect those systems now, your company can expect continued success, productivity, and profitability.

Other Telecommunications Recovery Concerns

Telecommunications disasters can be particularly insidious toward the successful activation of a disaster recovery plan. It can be next to impossible because the disasters often affect the phones themselves! Consider how your plan will operate if in fact there is no telephone service at all.

First, from time to time, disruptions occur in the switched public telephone network as a whole and have no individual cause in the way of a hardware or software failure. Many times, the demand on the network just exceeds the capacity of the network.

For example, as soon as the ground stops shaking immediately following an earthquake in California or in another area, one thing that typically happens is, you pick up your telephone to call your neighbor to say, "Wow, did you feel that?," and guess what, there's no dial tone! In fact, there's no dial tone for quite some time. This is because thousands and thousands of users picked up their phones as soon as the ground stopped shaking to do the same thing that you did. Contrary to public belief, there is no God-given right to dial tone!

Dial tone is, in fact, engineered on a shared basis. For example, in residential areas, it is very typical to engineer a 30:1 of dial tone senders to actual subscribers. In business areas, this ratio may be as high as 8:1, but it's still technically a shared resource.

For example, you're reading this book at this moment. What's your telephone doing? Nothing! This allows the resource provided for your phone to be used by someone else who is at this moment speaking on the phone.

It would be extremely cost prohibitive to provide one-on-one dial tone for everyone. However, from time to time, the network does become saturated. One such instance might be when a radio station hosts a contest and thousands of people make attempts on the network at the same time.

If, at any time, in an emergency situation, you lift your phone and there is no immediate dial tone, just wait. It may take 30 to 60 seconds, but eventually, the dial tone will come on. The way you can identify this condition from a dead line is that when you lift the phone, you should still have voltage for your touch-tone keys, and the phone should still sound like a live line. There just won't be any dial tone. If you lift your handset and the line sounds completely dead, there's probably another problem with the line.

When a major telephone serving office has a disaster, it affects far more these days than just local dial tone. A local telephone office provides dial tone to a 35-sq-mi or more area of town. End offices also provide an awful lot more these days than just dial tone. They provide access to wireless carriers and paging companies to name just a few. Depending on where you are, you could lose wireline and wireless phones.

End offices also carry a great deal of tandem traffic, i.e., traffic that switches through a CO on its way to somewhere else, to a user who does not live or work in the serving area of the CO through which it is switching. Back in "the old

days," only Class Four and above COs switched tandem traffic. Today, as in a lot of things, however, the old Class Five, or end offices, have much higher-level functionality. The network also looks much more like a peer-to-peer configuration than the old Class One-to-Five hierarchy. Now, even small switches can provide services that, in the past, could only be provided by higher-level switches.

What this means is that in a disaster this may happen: When was the last time you picked up your phone, dialed a number, and got a recording that said, "I'm sorry, all circuits are busy now. Please try your call again later." That happens to everyone, I believe, from time to time. How many of us really wait until later? Typically, I hang up and redial right away; that's "later." And most people do the same thing.

Call processing is based on something called the Erlang Theory. Erlang Theory is based principally on two things: call attempts on the network and call duration. Let's say that a user typically makes 30 calls per day during a business day. That's usually just 30 attempts on the network. And, let's say that the average length of each call is 3 minutes. If this is the profile of the typical user, a Telecommunications Manager or Network Engineer can take this information, multiply it by the number of users, and decide the number of trunks, tie lines, dial tone, or whatever he or she needs to accommodate these users.

Telephone companies do something very similar to this. Networks are engineered to provide a very high level of service but on the average amount of usage on a given business day. When a key telecommunications hub is taken out of the picture, some of the paths for completing calls through the metropolitan area are taken out.

It's impossible to determine what the outcome of this will be because we don't really know what time of day the disruption will occur, where it will occur, if diverse paths will be available, and if so how many. Or even what the load on the network will be at that time. There are a few things that are predictable. Users will begin to be blocked, so again, when the number is dialed, and the user gets the recording "I'm sorry, but all circuits are busy now. Please try your call again later," the user tries again immediately. When the user gets the recording a second time, he tries again, and again, and again, and again, until the call is successfully completed. What would have been one attempt on the network has suddenly become six.

Let's look at the other side of Erlang Theory: call duration. If I've just dialed six times to get another telephone subscriber on the line, I'm going to be very reticent to give up that line for fear that I will have to go through the entire process again. So, my first words to the person I'm calling may be, "Gee, Bill, are you having telephone trouble? I had a hell of a time getting you on the phone! Let's be sure we have absolutely no more business to conduct before I hang up, because I don't want to have to do this again!" When this happens, what happens to call duration? Exactly, call duration increases exponentially.

Now, the next user trying to access the network may have to dial seven or eight times. Depending on when the disruption takes place, this snowballing effect, if

you can call it that, means that a serving wire center, which normally only switches perhaps 10 percent of the tandem traffic in a given day, might, in fact, cause 75 percent or more of the calls to become blocked on the first try. Even the time of day when the disruption takes place has a bearing on the severity of this phenomenon.

Most people have seen graphs that show the typical call distribution level within a business day (see Figure 7.2a). Picture a graph with the level beginning at 8:00 A.M. and ending at 5:00 P.M., with two distinct humps in the middle. For example, at 8:00 A.M., people begin to arrive at work. But, they don't go to work right away. They stand around the coffee pot, talk about last night's game, wander over to the office, and eventually begin to settle down into their routine. At 9:00, of course, the boss comes in, and so traffic picks up. This peaks at around 10:30, statistically, with most companies. Around 10:30 to 11:00, employees begin to think about lunch, and gradually the traffic tapers off, and subsides somewhat around the lunch hour, typically between 11:30 A.M. and 1:30 P.M.

The typical employee leaves from 11:30 to 12:30. However, the boss, as everyone knows, takes two hours; so the traffic doesn't begin to really pick up again until about 1:30. Then, we hit another smaller peak around mid-afternoon, in the 2:00, 2:30, 3:00 time frame, which gradually subsides throughout the rest of the business day and then cuts off almost entirely at 5:00 when people go home.

Now consider wireless patterns (see Figure 7.2b). In general, they run just the reverse! The peak periods are when people are in their cars, or when those "free minutes" kick in after 7:00 or 9:00 P.M.

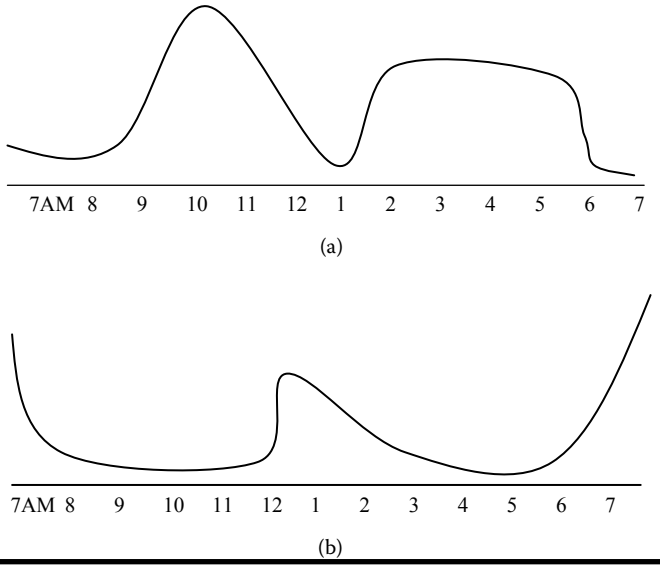


Figure 7.2 Call distribution: (a) typical wireline call pattern, (b) typical wireless call pattern.

Even though I made a few jokes during this illustration, this is, in fact, a statistically verifiable traffic pattern for most businesses. Because we can never tell what time of the day a given telecommunications problem will occur, such as a cable cut, it becomes even more difficult to predict what the effect on the network will be. If a disruption occurs at 3:00 A.M. in the morning, we may not be aware of it because everyone would be asleep. If the disruption occurs at 10:30 a.m., in the middle of the peak business day, everyone will be aware of it and demanding restoration of service at the same time. These are a few of the reasons why network engineering, Erlang Theory, and other tasks associated with telecommunications management can be both interesting and baffling.

Wireless phones have a very useful place in any disaster recovery plan for maintaining command and control. The wireless telephone network is, in effect, a gateway to another serving wire center. A company experiencing an outage, either due to a cable cut, CO failure, or other cause, can often restore critical functions via cellular telephone, with a few qualifications. First, wireless is a finite media, meaning there are only so many send and receive frequencies available in a given area or cell. Second, wireless does have a speed limit, typically, for data, and it's generally at modem speeds.

A user expecting to back up a telemarketing center of 200 people using a pile of transportable wireless phones is probably in for a rude shock. However, there are a few things that can be done to partially mitigate this problem through the use of micro-cell technology. A micro cell is a piece of equipment not unlike the cell sites that dot the landscape throughout the metropolitan area. In this case, however, this particular cell site is a smaller, lower-power version that is dedicated to a single user or to users within a given building. Two types are available. One is normally used, for example, in hospital environments. A direct microwave connection is established from the user's location into an MTSO (mobile telephone switching office). This microwave system is then terminated in a micro cell, the output of which provides two wire ground-start trunks, just like the Voice Communication Manager is accustomed to getting from the phone company.

In the event of a major cable cut, for example, the PBX equipment is smart enough to sense the loss of some of the trunk and begin routing the traffic over the available trunks, i.e., the micro cell. The traffic goes out over the cellular network without the user even being aware that it's happening. This works very well, except in cases where the actual PBX is disrupted in the disaster. In these cases, another technique is used, where an antenna, commonly called a "leaky coax," is strung between floors in the building. Users then use regular handheld cellular phones to bypass the crippled PBX, again completing calls over the micro cell to the MTSO (see Figure 7.3).

Cable Cuts! How to Protect against Them

Despite advances in protective technology, for most companies the cable cut is the most common cause of telecommunications disruption today. In my 30-plus

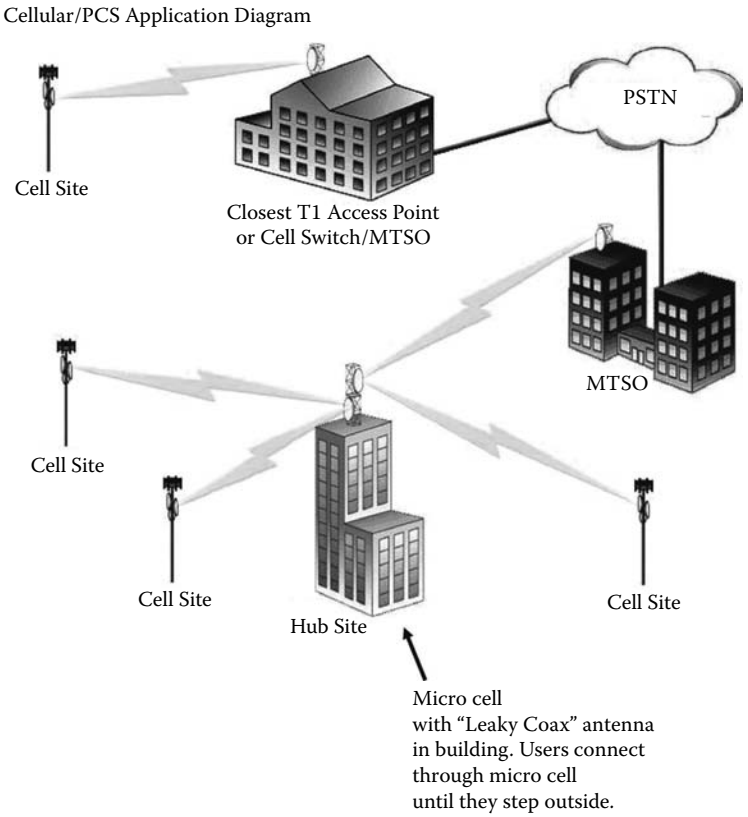


Figure 7.3 Cellular/PCS application diagram.

years in this business, I have yet to find another telecommunications user who has not experienced one. Think back for just a moment on the FMEA (Failure Mode Effects Analysis) methodology we discussed in Chapter 3. Remember that a FMEA is based on severity x frequency detection. How severe is a cable cut? Oftentimes, it can isolate your facility entirely from the outside world. How often does it happen? Pretty often, or at least often enough so that everyone has experienced one. What about detection/resolution? Many times they last all day. It is not at all unlikely that gas lines, electric lines, or other type of services may have been cut at the same time. Because some of these present hazards such as gas and electricity, frequently telecommunications services have to wait until the electric and gas companies are finished. Another common occurrence involves communications facilities that are installed underground, adjacent to railroad tracks. When a train derails, it can play havoc with these facilities, and if it spills a load of ammonia at the same time, delays can be considerable. My point here is that cable cuts are severe, happen regularly, and sometimes take a long time to repair. Because you are planning for something

that will happen (rather than what might happen), shouldn't this item be placed high on the priority list for resolution? I personally think it should.

Immediately following are a few things you should know about why cable cuts happen and how you can prevent them. Later in this chapter are some advanced tips, such as the installation of fault-tolerant fiber-optic rings and other technologies, which, if installed properly, could mitigate this risk for good.

1. First, consider where everyone lays cable. Virtually all cables, whether fiber optic or copper, utilize long stretches of real estate along railways, roads, and easements. These are called *public right-of-way.* When telecommunications companies build facilities, it is far too expensive to negotiate with each and every home and business owner to cross their property. That's why most, but not all, properties have special easements along the edges earmarked for use by the utility companies. I say most because this is not always the case. When I was a city official, for example, we needed to build a water line down what we thought was a fairly major thoroughfare. As it turned out, one single piece of property owned by a concerned tree lover abutted the road but did not have a utility easement. This woman would not let the city's contractors dig for fear it would kill her oaks. Anyone who has ever been through these negotiations knows what a pain they can be. A few thousand dollars later we had the easement, but we had to buy it and also give the property owner a warranty on her oak trees for a year against damage. That was only one instance on one street. Multiply that by thousands for a telecommunications company that wants to install facilities, and you get an idea of the problem. Sometimes, it is easier for utilities to condemn properties and invoke public domain to get access to right-of-ways, but that's a topic for another book. In any event, because of this, right-of-ways tend to be crowded, used by multiple vendors, and are likely to girdle something that is already in place such as a street, railroad line, or highway.
2. Unfortunately, in many cities, there are right-of-ways that have been in use for many, many years. When someone starts digging, they never really know what they are going to hit on the way down. Obviously, construction activity is common along roadways. The issue is even more complicated when one considers that gas, electric, and sewer lines traverse the same right-of-ways. Gas lines get cut, as do electric lines. Somehow, I don't see a lot of sewer lines getting cut. I wonder why?
3. Each kind of right-of-way has its own inherent risk. Trains derail and cut cables. Road crews dig adjacent to roadways. Sometimes crews don't want to dig up the street, so they use machinery to "core" under them. In the process, they may core through a cable on the other side of the street. Farmers and homeowners drill fence posts at the edges of their property, often right through cables that traverse the right-of-way. In fact, the issue is so prevalent that virtually everyone in the telecom business has his or her favorite

> cable-cut story. Years ago, when I was at AT&T, thousands of people in Dallas lost service for most of a business day. The source: a farmer burying a dead cow — and in the process digging up AT&T's main cable route. Or, consider the case of the outside cable supervisor in New York City who told his new technician, "There are two fibers down there in the manhole. Cut the BAD one …" New York was isolated for most of the day.

There are things you can do to mitigate your exposure to cable cuts. The first step might be a meeting with your local telephone company. They can provide you with helpful information if they take the time to do a little homework on your behalf. If you have an account manager who is not all that knowledgeable, have that person seek out a SME (Subject Matter Expert) with experience in network engineering and protection. The local telcos really do have these people, although you sometimes have to seek them out.

Can Alternate Cable Routing Be Purchased from the Telco?

Many times alternate or diverse cable routing is available in your company's service area for little or no cost. First, however, let's get the terminology straight. A lot of people use the terms alternate and diverse interchangeably. They are not the same things. Generally speaking, alternate is anything other than the configuration you have now; Diverse implies a totally separate and physically diverse path. *Alternate* might mean a different "100-count" in the exact same cable. *Diverse* should mean at a minimum, a completely different cable, and if the engineer knows what he or she is doing, a completely different right-of-way, too (see Figure 7.4).

Other technical terms you can use to converse with these folks include *count diversity*. Count diversity is, as I mentioned earlier, where different "100 counts" in an existing cable are utilized. So what good is that, you might ask? The answer is, not much, except for one case. Have you ever had a circuit or number of circuits disconnected in error? Count diversity in some situations could reduce the possibility that disconnection will happen because the cable appearance will be on two separate physical connection blocks in two different locations on the distribution frame in the CO. Another common term is *sheath diversity*. Sheath diversity uses separate cables but still in the same conduit and manhole.

Other types of diversity can include items like *nonadjacent ducts*. A lot of cable, especially in the cities, is not directly buried but lies in ducts beneath the street. If you ask the telco engineers to place the multiple cables serving your enterprise (assuming there is more than one, as this is not always the case) in different ducts, you could buy yourself a little more protection. This is based on the idea that a backhoe operator will have the brains to stop digging when the backhoe hits the first cable, presumably near the surface. If some of your service is in deeper or nonadjacent cable ducts, you might not lose everything. Even so, there was an incident when I was at AT&T where a backhoe operator hit the concrete case that protects

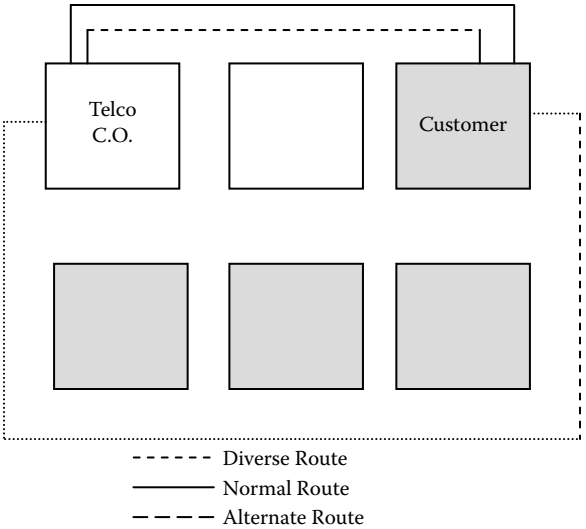


Figure 7.4 Know the difference between alternate and diverse routing.

the ducts. He thought it was white rock, which is prevalent in North Texas. So what did he do? He "whaled" on it, smashing it repeatedly with the equipment. First, he broke the water line, then he cut the electricity, and then he heard a hissing sound. Backhoe operators know what the hissing sound is and, lucky for him, he got out of there just in time before the explosion. What resulted was a three-day telecom outage for many people in the area. This is because, first, the providers involved had to fix the gas, then the electricity and the water, and finally the telecommunications cable. (At least, I think that's the order). Further, they all had to coordinate, which as you can imagine is a challenge with no less than four separate companies.

What Is at the Other End of Your Organization's Telco Cable?

For most companies, the "other end" of the cable — and the first point of physical vulnerability other than the cable itself — is the local telephone serving office for their area. In most cases, all data and voice traffic must pass through this location as the first leg to wherever it is going, whether across town or around the world. The physical capabilities and configurations of these local offices vary greatly.

In our 1993 book, coauthor Eddie Pope and I wrote a great deal about fiber-optic rings, SONET (synchronous optical network) technology, and some great "Buck Rogers" technologies that would make cable cuts a thing of the past for everyone. It has not quite worked that way. To give the telco credit, the public switched network is a lot more resilient these days. The old hierarchy of the numbered class COs has been largely abandoned in favor of linking multiple COs together in more of a peer-to-peer fashion. That's why there are fewer "all circuits busy" recordings

these days. A decade ago, a cable cut all the way across town could affect you by saturating the unaffected portions of the network with calls. That can still happen today, but it's generally not as bad because the metropolitan networks have more alternate and diverse paths for calls. Dedicated circuits, however, are another matter (see Figure 7.4).

So are services used by Competitive Local Exchange Carriers (CLECs) and some wireless providers. We will get to those issues in a moment. Getting back to what a CO is and how it is vulnerable:

Most local serving offices are sound structures that are constructed of reinforced concrete. Because designs vary, you should drive by the serving office. Look for the obvious. Does the structure have a large portion of the surface area covered by windows? Does it appear to be in an area prone to flooding? Is there major construction activity planned or occurring in the immediate area around the CO? Ask some questions of your telephone company's account representative. Is the CO manned 24 hr a day? What type of fire prevention systems does it employ? How old is the structure?

Interesting Ways to Interview the Telco and Assess Vulnerability

One item most operating companies are quite willing to provide is a CO tour on request. There is one reason that is more important than any other (it often includes a free lunch!) to request a tour. That is the ability to meet the people who install or work on your circuits face to face rather than just on the phone. This helps smooth out day-to-day operations and establishes an atmosphere of trust where you can learn more about what the telco does for disaster recovery. Some good questions to ask might include:

1. Is the CO a tandem or end office? End offices serve only end customers. Tandems switch traffic from one end office to another. Many COs presently perform both functions. This could have a bearing on which systems get recovered first in a disaster, as well as how many people might be affected in a metropolitan area. For example, loss of a tandem all the way across town could still affect you by contributing to network congestion and blocking your calls.
2. What plans exist for restoration in the event of fire and flood? What services would be affected?
3. How difficult or expensive would it be for facilities to be brought in from another CO? Occasionally bringing in alternative facilities is reasonably straightforward, but done often, it is prohibitively expensive, if not impossible.
4. Try to get an idea of the topology of the entire city's telephone network. Is it a hub-and-spoke or peer-to-peer configuration? Hub-and-spoke is more

economical for the telephone company because facilities are better utilized. It is not as reliable, however, as peer-to-peer, where alternate routes for switching are more likely to exist (see Figure 7.5).

5. Ask about the location of the regional serving offices and access tandems. As I stated earlier, you may find that many CLEC, long-distance and wireless companies are congregated in just a few "carrier hotels," or that they derive all of their connections to the Bell network in the same access tandem downtown. This is not always the competitor's fault; in fact, often it is the Incumbent Local Exchange Carrier (ILEC) that makes the competitor accept less-than-optimal connections.
6. For example, frequently, the monopoly ILEC makes it difficult for competitors by making switch diversity, ROTN (Route Other Than Normal) cable routing, fiber-optic ring technology, or "dark" fiber cost prohibitive or difficult to get. You will obviously get two different stories on this issue, depending on whether you are speaking to the incumbent monopoly or competitor. One thing is certain: the interconnection agreements (ICAs) used by competitors to connect its networks to incumbents like SBC (AT&T) in 1997 contained dark fiber, SONET rings, T1 loops, and other technology to bolster network integrity. Today the ICAs do not contain such provisions due to lobbying of the FCC by the incumbents. That means either the competitor has to build

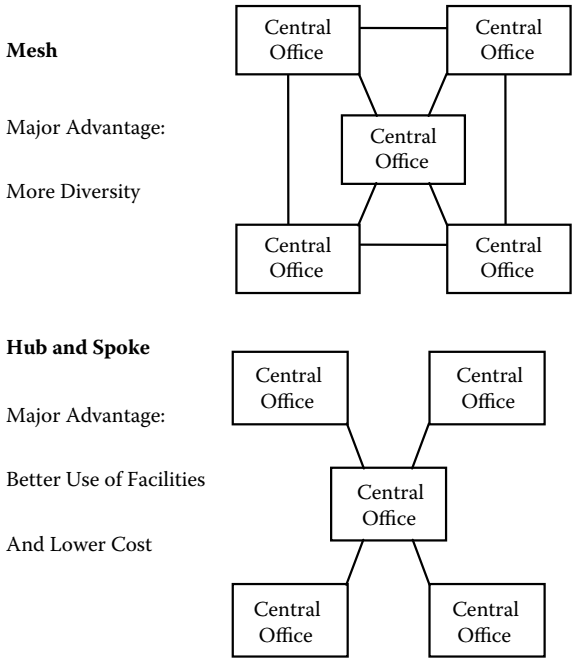


Figure 7.5 Understanding the telco network and how it could affect you.

its own facilities (an expensive proposition) or your firm may be forced to go back to the monopoly. There are a few bright spots, however. Wireless services are making a comeback, and are discussed later in this section. They are inexpensive and provide a great alternative for connection to carrier hotels and other points of vendor concentration.

Physical Vulnerability to Telco Disasters — Where Does One Start?

The size and density of the serving area for the office vary substantially from one serving area to another. So, where does one start and how does one prepare? First, you might consider taking a drive to find the site of the local CO for your area. It should be no more than a few miles away, with very few exceptions. In the center cities, it may be only blocks away. Out in the country, it could be miles away. Suffice it to say, however, that probably 90 percent of them are within 18,000 cable feet or less of a subscriber, or less than 3.4 miles. Once you have located it, drive the route between it and your company location. Look for construction, digging, or other activity in the right-of-ways along the street. After a while, if you are so inclined, you will even learn which boxes and pedestals contain fiber-optic equipment, xDSL equipment, T1 repeaters, and other components. It is not as though any of this is going to help you do anything about potential disasters, but if you spot a big construction crew working adjacent to your company's fiber terminal, you can at least have some possible warning that something may happen. Another easy way to become familiar with the service area of a particular local CO is to pick up a local telephone directory and look at the first few pages. Sometimes, but not always, there is a diagram that illustrates the local calling area and exchanges served in the immediate area. The scale may not be exact, but it gives a good indication of the relative size of the service area. It might even list the telephone prefixes (NXX codes) for the area. By comparing this diagram to a regular city map, it is possible to get an idea of how many other companies are served out of your area's local telephone office. This could have a bearing on recovery time in the event of a severe CO outage. You can also get an idea of how far you would have to drive to find a working phone if the CO is destroyed or incapacitated.

Although this diagram is a good starting point and serves as a general overview, there are other better and more detailed references available. One such source in the United States is the Public Service Commission (PSC) for each state. The PSC is repository of a wealth of information on this subject for those willing to do some "digging" — in the sense of research that is, not backhoes. Local exchange companies are required to file detailed maps, diagrams, and other information regarding their franchise areas on file with the individual state PSCs.

Useful data on file can include the following:

1. Definition of the serving area for every CO in the state, down to the particular street. For example, not only will the larger cities be served but all or some nearby towns and parts of others.
2. Distances to other serving offices can often be approximated through the use of available documents, which could be important for companies considering diversity through special construction of facilities at another serving office. Quite naturally, the cost of such a project will vary with the distance and availability of existing cable or fiber.
3. Distance, however, is not the only consideration. The closest CO, for instance, may not contain the technology needed by the customer. A different local operating company — a difficult prospect in both the construction phase and in future circuit coordination — may even operate it.
4. Information can be secured from the public service or public utility commission for the cost of making copies of it. For the address of your commission, take a look at http://www.naruc.org (National Association of Regulatory Utility Commissioners) and then click the button that says "about naruc," and then click on "State Commissions."

Wireless Services as an Alternative for Protection against Cable Cuts

An increasing number of wireless technologies are becoming available that are useful to large, and sometimes even small, organizations for network diversity and disaster recovery. Technologies such as microwave bypass have been available to large organizations for years. Today, however, even small companies can get in on the action through the use of P-P (Point-to-Point) or Point-to-Multipoint (P-MP) technologies, which scale down even to the level of individual households. The office of TellawCom Labs, Inc., for example, where Leo resides, generally has no more than five or six employees, yet it has a diversity of telecommunications facilities. Some come in on traditional landlines and others (voice and data) use wireless. There is no reason that some of these technologies should not be in use in your own organization's network to protect yourself against the failure of a service provider or other calamity such as a cable cut. Thoughtful engineering and pre-selection of numbers essential to command and control after a disaster go a long way to assuring that your plan executes smoothly.

Wireless technologies can include mediums such as the following:

- Infrared point-to-point links
- Microwave radio
- Satellite communications
- P-MP systems (unlicensed)

Each has its own inherent strengths and limitations. The application for the technology you choose to back up (voice, bursty data, Internet, etc.) also plays a role in selection of a technology. For a variety of reasons I like P-P as my wireless disaster recovery alternative. First, as I stated earlier, I have some hands-on knowledge of the technology by virtue of using it in my own office. There are also a lot of other benefits to it. These include low initial start-up costs, a high degree of flexibility and interfaces, much higher potential throughput speeds, and the fact that these systems do not have to be licensed.

In the following text, I begin with a brief summary of some common wireless alternatives to establish the context, show what else is available, and what the pluses and minuses are in any wireless implementation. Let's start with infrared links.

Infrared Point-to-Point Links

Point-to-Point infrared links are not really radio but invisible light, a conceptual cousin to the infrared remote control for your television. Advantages include the fact that they are inexpensive, do not need to be licensed, and come with a variety of interfaces including T1 and Ethernet.

Infrared requires line of sight, i.e., one end must be physically visible to the other end of the link. And because these systems operate in a much higher frequency range than other alternatives (light, even infrared light, operates in the terahertz range, whereas radio operates in the megahertz or gigahertz range), there are distance limitations as well. Infrared is also much more affected by fog, rain, snow, birds, and, practically speaking, anything that will interfere with the propagation of light.

On the other hand, the equipment is compact and does not require licensing. The equipment can easily be mounted in a building, does not require any special power or environment, and the transmitter/receiver can operate through window glass with few problems. If you have an application that requires you to get a T1 across the street or across a small campus, Infrared may be your least expensive solution (see Figures 7.6 and 7.7).

Infrared systems are also often used for LAN interconnection in buildings that are in close proximity but separated by public rights-of-way (such as streets), where cabling between buildings is impractical. If you consider the use of an infrared link yourself, be sure you don't exceed a mile or so (less, if you are prone to periodic fog or heavy rain), and that you have clear line of sight.

Interestingly enough, I have run into several cases where the line of sight becomes an issue. One user we worked with had a clear line of sight to a neighboring building all winter long. In spring, however, when the leafless trees on his property line sprouted, the new leaves blocked out his infrared link. Another user lost service periodically every time the window washer came by on his high-rise building. This only happened now and then, and he moved on quickly, so it was no

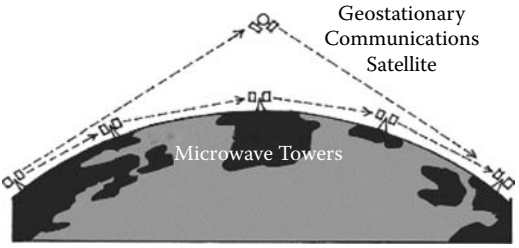


Figure 7.6 Satellite communications.

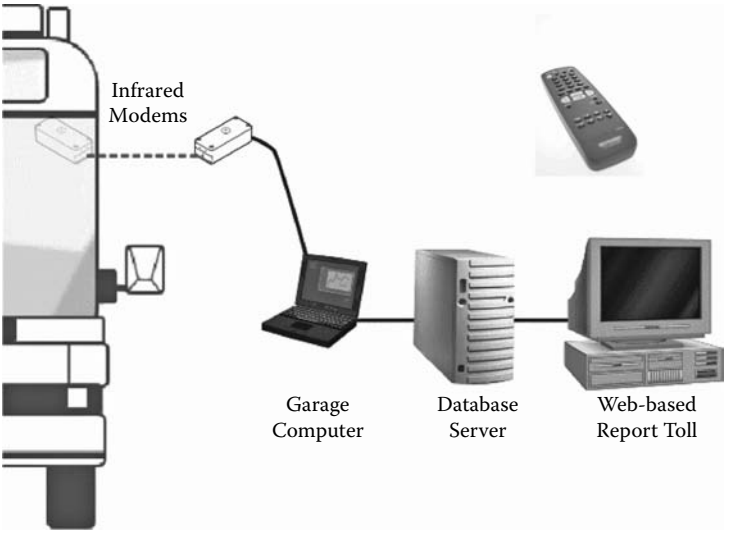


Figure 7.7 Example of infrared technology: remote control for your TV.

big issue. On one such pass, however, the window washer happened to leave behind a large streak across the window, which — as luck would have it — refracted the light just enough to cause problems with the link. They had to get the window washer back out the next day to clean off the smear. Despite the limitations, the cost, diversity of applications, ease of use, and the fact a license is not required still earn infrared links good marks, subject to the concerns expressed above.

Microwave Radio

Microwave has broad applicability, high reliability and availability, relatively good ease of use, and relatively low cost. On the negative side, you do need a license to operate most microwave systems, and the more popular frequencies are congested and difficult to get licensed, especially in the major cities. Microwave

started originally as a telephone company technology. The telcos especially liked the ability to span bodies of water, valleys, and other terrain without having to lay cables. Indeed, until the 1980s, AT&T still had microwave links in its network (maybe they still do), some of which spanned mountain top to mountain top at distances of 30 mi or more.

Satellite
Microwave
007x015
Infrared
P-P Microwave
P-MP Microwave
Other Wireless Technologies

Like infrared, microwave requires line of sight. This is problematic within major cities. If you are lucky enough to get a frequency licensed, all of your work could be undone because someone builds a building between the two points on your microwave link. This problem occurs more often than you might think.

Microwave enjoyed most of its popularity in the 1980s as a "by-pass" alternative to go around the local telephone companies. At that time, the "last mile" of circuits (known as "loops") got expensive; at the same time, long distance got cheap. The logical response of enterprise users was to dump the local telephone company and use microwave to connect directly with long-distance carriers like MCI and Sprint. Although the financial motive was the primary driver, it only took enterprising users until their next cable cut to realize that microwave also had use as a disaster recovery technology. Microwave provided the ultimate diverse route because one cannot dig up air.

As a general rule, the higher the frequency of a microwave link the shorter the path must be. I have personal experience with installing a 2-GHz (gigahertz or billion hertz per second) link a number of years ago. This link was rock-solid on an 8-mi line-of-sight for years, until the 2-GHz band was phased out by the FCC for another wireless technology. Afterwards, it was replaced by a 6-GHz link that boasted comparable reliability. Another popular frequency is 23 GHz, but it has more of a tendency to "wash out" in a heavy rain because a higher frequency is more easily absorbed. Even so, it has been more than a few years since I had actual "hands on" contact with these technologies. I would not be at all surprised if 23-GHz performance rivaled what we achieved years ago with 2-GHz systems, simply due to advancements in microprocessor and antenna technology. Check with the manufacturer and stay within the design limits of the equipment, and you should be fine.

As microwave has gained favor with enterprise users over the years, the feature richness and reliability has increased. Many systems today employ fault-protection switching, which is, in effect, two radios in one. When one fails, the other cuts in almost instantly with no interruption in service. There is also a greater choice of interfaces today, with Ethernet and T1 interfaces commonplace.

As stated earlier, however, you will be required to secure an FCC license to operate a microwave system. The manufacturer can help you do this, and there are also numerous consultants that can literally be found in the yellow pages to help you with it. If you are looking for true diversity at a reasonable cost and at higher reliability than infrared, microwave may be the ticket.

Satellite Communications

This discussion would not be complete without a brief overview of satellite communications. Like the previous two technologies, satellite communications have taken leaps and bounds over the last few years. Satellite is essentially microwave radio aimed upward; it uses essentially the same frequencies. As such, the same rules hold true regarding tendency to wash out. There are also two times every year when the satellite receiver will be aimed directly at the sun, right around the spring or fall equinox. At that time, there will be a brief outage. These can be planned for, however, because the service provider will know precisely when they will occur.

Satellite has gone from elaborate teleports and 16-foot dishes in years past to pizza pan dishes that fit on the side of a building to (in the case of Global Position Systems and freight-tracking technologies) units that literally fit in your hand. Notwithstanding timing delays (it takes a significant fraction of a second for the signal to go from the earth up 22,300 miles to a geosynchronous satellite, and the same distance back), satellites are a clean, reliable, and cost-effective disaster recovery solution. (See Figures 7.6, 7.7, and 7.8.)

It is interesting to note that some companies' enterprise networks are virtually 100 percent satellite already. It is probably prudent, therefore, in these cases to explore another technology for backup. Even the military does this. In the 1970s the dominant technology used outside the United States was something called

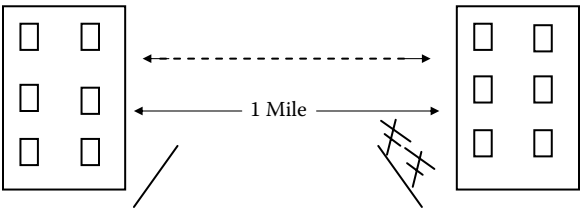


Figure 7.8 Example of infrared technology: building-to-building network interconnection.

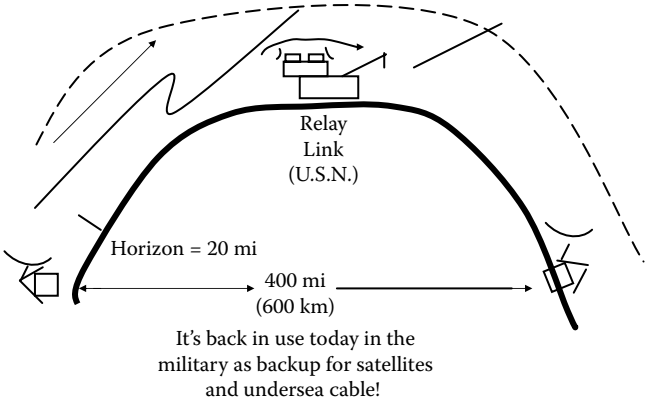


Figure 7.9 What is tropospheric scatter? (Tropo).

tropospheric scatter radio or just Tropo. Tropo blasted a very strong signal at the horizon. Most of it went out into space. Enough of it, however, "bent" over the horizon to allow communication between bases or ships without the two ends having to have line of sight. Today's war planners have contingencies for loss of satellites because these would be obvious targets (the earth stations, at least) in a conflict. The backup technology for satellite technology is Tropo. For other satellite users like network television, it is landlines (see Figure 7.9).

It is probably not practical for your company to license and install a Tropo system, but even so, there are ways to back up satellite with other technology, such as land lines.

One limitation of satellite technology is with certain voice communications services. A geosynchronous satellite orbits 23,500 miles above the earth or about a 50,000-mile round trip for a conversation. Light travels at 186,000 miles/second. On paper, at least, that equates to a little over a quarter of a second of delay. That's enough to become noticeable before one even considers other things that can slow a circuit down, such as latency in IP and other protocols, as well as capacitive reactive components in circuits that can also add delay. The effect of this becomes apparent in the following example, in what I consider to be my all-time favorite telecommunications practical joke: letting someone in the shop talk to himself or herself. It goes like this.

While at a gateway AUTOVON (Automatic Voice Network) hub in Japan in the late 1970s, we had access to the Model 490L AUTOVON switch. (Boy, now some of you really know I am dating myself!) The switch was connected by interswitch trunks to other switches worldwide. We would begin by jacking in directly to a satellite trunk from Japan to one of the international gateway hubs in California. From there, the call would progress via the commercial AT&T network across the United States to one of the international gateway hubs on the East Coast. There was actually nothing in the network to prevent its picking up a second (or, sometimes a

third) satellite hop at this point that terminated in the United Kingdom, Germany, Turkey, Italy, or anywhere else we had another switch. We dialed up a loop back.

The call then traversed two or three satellite hops from Turkey all the way back to Japan. By the time it got there, there was a delay of two or maybe three seconds if we got a good one. We would then ring the patch to the home of any supervisor who, at that particular moment, was not held in high esteem. At 3:00 a.m., picture the scenario:

Hello? (Silence)
Hello? (Silence)
Hello?

He was about to hang up, but then his "hello" comes back at him. On a 1970s vintage analog circuit going 100,000 mi, he could not tell it was his voice; only that it sounded like an international call. The next two or three minutes were invariably hilarious as the poor victim tried to establish contact with himself!

Victim: Hello? Response: Hello?
Victim: Who is this? Response: Hello?
Victim: Who is this? Response: Hello?
Victim: Who is this? Response: Who is this? (Now the "who is this" is coming back!)

After a few minutes of this, they eventually figured it out and went back to bed, but during the time it was up, we would usually have it on a speaker in the shop for everyone to enjoy. It was funnier than Abbott and Costello's *Who's on First* routine.

I have two points to be made here. One is obviously that delays in satellite transmission can impact voice communications. Second, consider the security implications. Note that I said we could monitor the line on a speaker. Anyone can. If it goes over a wire or the air, it can be monitored.

P-MP Systems

The challenges of setting up an effective primary and disaster recovery system have always involved trade-offs between cost, complexity, reliability, and time (such as in licensing). Concerns about designing, installing, and maintaining complicated networks and unfamiliar technology also drive the selection process. In many ways, this makes the newest entrant of the technologies discussed in this article, P-MP, the technology of choice.

P-MP marries microwave radio technology to enterprise communications applications, and in many ways makes deploying and delivering telecommunications technologies of all types faster and easier than ever before. P-MP provides the performance, versatility, ease-of-use, and affordability that enable enterprise

environments, including corporate, municipal, healthcare, education, and more, to improve communication, productivity, security, and return on investment (ROI). This technology is also becoming widely used as a disaster recovery technology. Indeed, two users that we are familiar with, both of which are county governments, have scrapped its AT&T T1s altogether and now use P-MP as the primary technology, with a few T1s held back as the backup path.

Here is how the technology works: P-MP products operate in the 900 MHz, 2.4, 5.1, 5.2, 5.4, and 5.7 GHz frequency bands. As these frequencies are lower than many microwave frequencies, "wash out" and restrictions on range are not as much of an issue. Like the other technologies, a variety of interfaces are available including T1 and Ethernet. Start-up costs are low. We have seen central unit costs as low as $2500 and "per rooftop" costs in the $500 range. Typically, a small antenna (about a foot long and four inches wide), or in cases where the range is greater, a small dish about the size of a satellite TV antenna, is installed on the roof.

The need to run cable is thus obviated. The equipment also does not require an FCC license. The equipment itself is streamlined, with the radio built into the antenna in the same 12" × 4" × 2' unit on the roof. It's very easy to get up and running. Most P-MP platforms also include the most common interfaces that enable them to easily integrate with standard network management tools and systems.

Obviously, any system that traverses an airwave should be encrypted. Look for a system that provides security with over-the-air DES (Data Encryption Standard) encryption or AES (Advanced Encryption Standard) encryption capabilities.

P-MP systems serve numerous enterprise locations of virtually any size and can be used for distances up to 15 miles (24 kilometers). P-P links can traverse much greater distances by augmenting the antennas at both ends (a dish similar to a microwave dish is used in these cases), and these, in fact, approximate the "mountain top to mountain top" links described previously.

Most P-MP systems require line of sight, although some of the ones that use the lower frequencies (like 900 MHz) do not. The lower frequencies, however, generally limit throughput to T1 speeds (1.544 Mbs), if you are lucky.

To summarize, P-MP systems, in the opinion of this writer, represent the best trade-off in cost, performance, ease of use, and variety of interfaces available to the enterprise user seeking disaster recovery and network availability:

Easy to Use

> Most P-MP equipment is intuitive and efficient, providing built-in installation and deployment assistance that makes it faster to get up and running … often in a matter of hours or days instead of weeks or months.

Flexible Options, Good Distance, and Numerous Standard Interfaces

These can be configured as a single-site P-MP system that supports subscribers for distances up to 15 miles (24 kilometers). It includes common interfaces that enable it to easily integrate with standard network management tools and billing systems as well as the diagnostic capabilities you'll need to remotely monitor the network or reconfigure in a disaster.

Security Straight out of the Can

Most systems are available out of the box with security including over-the-air DES or AES capabilities, which provide 128-bit encryption. One vendor claims that, with AES, it would take approximately 149 trillion years—that's older than the earth itself—to crack a code.

Increased Speed Dividend over T1

Upload and download speeds are as fast as or faster than that of many services available today. A typical P-MP system can offer speeds from 512 Kbps to 14 Mbps, and P-P systems can deliver from 10 to 300 Mbps. Two users we know of, both county offices, have dumped their T1s or relegated the T1 landlines to backup roles as the wireless option is so much faster. The largest concrete manufacturer in Texas has dropped its T1 network altogether in favor of a P-MP provider, Midlothian, Texas-based Air Canopy, Inc. (http://www.air-canopy.net). Air Canopy also provides consulting services and can be reached for more information at (972) 617-8889. Hundreds of other such providers also exist and are entering this dynamic market.

Summary

If you detect a bias toward the new unlicensed P-MP and P-P systems over other wireless alternatives, from one who has seen a lot of wireless technologies over his career, I would say you are probably correct. First, I have never cared for monopolies like the phone company, and I like to have the widest diversity of choice possible. On the other hand, because my time has become increasingly valuable over the years, the ability to install a technology without having to take a class, obtain a license, or design a whole new interface box is also important. In these respects, P-MP works great from a cost–performance and disaster-recovery perspective. Sure, there are negatives. P-MP is unlicensed. That means there is always the possibility that someone else's P-MP or P-P link will interfere with yours. Unlicensed does not,

however, mean unregulated. There are still FCC rules that may help even in these situations — all the more reason to talk to a reputable purveyor of these systems.

From a disaster recovery perspective, all I can say is, "This is cool." Imagine a unit you can have shipped in overnight that can reestablish a T1, nail up an Ethernet link, or provide you upwards of ten times the capacity of a P-P T1 — all without a license, or the need to go to a school, or the need to add yet another black box to interface with your network. This deserves a look.

Wireless technology of any type can help you further safeguard your network, make it more resilient in a disaster, provide a boost in network performance, and maybe even save you a few bucks in the process.

Callout of the Telecom Recovery Team

Now that we have discussed a few of the possible impairments to implementing a callout in a disaster, let's talk about the procedure itself. The actual callout of the staff can be accomplished in a number of ways. Remember, as this is a telecommunications disaster, we're talking about, telephone service may not be available within the area. Although the first choice should be to telephone the staff using the home telephone numbers documented in the plan, there must be backup features in the event that this means is not available. These might include such items as sky-pagers or cellular phones, for example. In the case of telecommunications or telephone companies, it may be wise to have several means of contacting employees — the first being the telephone, the second being sky-pagers or cellular phones, and the third, perhaps, even being HF radio systems or items of that nature for use in the event of a massive failure, such as an earthquake. The Telecommunications Manager may act as the Team Leader for the telecommunications team and conduct the initial on-site damage report. He or she may act as a member of the Emergency Management Team (EMT) and designate another person to coordinate on-site activities. In either respect, the initial damage report will need to be provided to the EMT within 90 minutes or some other pre-subscribed time from the notification of the disaster. At this time, the EMT will decide whether to activate a companywide disaster recovery plan or simply let the Telecommunications Department respond to the disaster on its own, while providing periodic reports of progress to the EMT.

Establishment of Command and Control

Upon arriving on site, the Team Leader's first concern will be to safeguard human life. The second concern will be to secure the building as well as possible while trying to ascertain the extent of the damage. The Team Leader will coordinate with other team leaders on site from other technical service departments, as well as coordinate with emergency services on scene, whether they are the fire department,

paramedics, or whoever. While a Team Leader is on site, additional members of the team will be addressing other aspects of the disaster recovery plan. For example, from an alternate location, such as a home or another company location, members could be calling telephone companies and vendors to set up the first key command and control numbers. These include activating numbers for the EMT, restoring the network control help desk number, rerouting incoming 800 service that is out as a result of the outage, and call-forwarding any local telephone service for key command and control numbers. Additionally, these people will contact long-haul carriers for redirection of any Backbone T1 Networks or critical LAN router links to pre-subscribe disaster recovery centers if one is used.

Telecom Department — Specific Tasks and Procedures

In the initial reaction phase of the Recovery Plan, there will be some immediate steps that should be implemented in rapid succession. These include:

1. Procedures for how to receive the initial disaster report
2. Procedures for notifying the EMT and staff
3. Procedures for conducting the initial damage assessment at the center. For example, what format to submit the report in, and how long after notification before the EMT will expect a report
4. Procedures for safeguarding human life and helping the injured, if this is the case, as well as coordinating emergency services

This may also constitute a corporate wide or simply a telecommunications disaster, in cases where the disaster affects less than the whole building and is confined to the Telecommunications Department. Whether this constitutes a corporate wide disaster will depend on the nature of the disaster, the extent of the disaster, the types of systems affected, and the mission-criticality of those systems. It is imperative that the Team Leader arrive at the site without delay to make a determination of the disaster for evaluation by the EMT. This entails a complete determination of the nature of the disaster, the extent of the disaster, which equipment is affected, and if possible, some idea of the cause of the disaster. The same procedures for securing the installation from possible theft, coordinating with emergency personnel, and helping any injured personnel will apply. The Telecommunications Manager or Team Leader will also request an on-site technical person for each major vendor of each system affected. For example, if the disaster affects a PBX, an ACD voice mail system, or other technical system, efforts will be made to contact the users of those systems. They will then be advised that their ability to perform their jobs could be seriously impacted — even to the extent of being unable to perform their duties — for the immediate future, or until the situation is corrected. Although it could be a real pain to provide periodic status reports to a lot of end users, it is better than their trying to call you, and it's always better to be proactive than reactive when

dealing with your users. The Recovery Plan should note any roll-in replacement plans or guaranteed equipment replacement plans to the affected equipment. If this is the case, you will want to contact the vendor and start this process rolling as soon as possible. Calls should also be made at this time to any after-the-fact disaster companies, such as BMS Catastrophe and various other cleanup companies, as well as the company's insurance providers, to notify them of the disaster. This should also be noted in the plan.

Remember that the fire department may still have control of the building if this is the case, or the building may be shut down by civil authorities due to its being unsafe after an earthquake or due to chemical contamination. Always remember, you may not be allowed into the building to conduct a timely damage assessment, and you may end up having to wing it without benefit of this type of information.

Contingency plans for what to do in the event the building is shut down should also be included in this part of the plan. The Telecommunications Recovery Team should be assembled after the initial damage assessment is made and the preliminary report is filed through the EMT— both on site to begin with the cleanup effort and also at any designated disaster recovery facilities.

Software Disasters

Disasters to PBXs, ACDs, voice mail systems, and other systems, however, may not be due to fire, flood, or other causes. They may, in fact, be due to catastrophic software failures. If this is the case, there may be a very different checklist of items to accomplish to quickly ascertain the cause of the disaster and recover the affected equipment. The same procedures will apply for notifying the Team Leader, putting the EMT on alert, and providing reports to the EMT. However, a different group of people may be involved in determining the actual cause of the disaster — whether it's related to equipment failure, some type of a software glitch, hacker attack, or virus infection. Procedures should be included in the plan, but first attempt to recover by use of a backup software copy. These procedures would include where to find this backup software copy (for example, it should be stored off-site) and for reloading this software to restore the affected system. There should also be procedures in the event the outage is due to a hacker attack — for example, through a remote maintenance port. These procedures should include written documentation on how to shut the port down immediately as well as how to contact law enforcement authorities to possibly trace the call. In the case of a virus infection, procedures should exist on where to find cleanup software, what software to use, and a procedure for both troubleshooting and eradicating any viruses that may be in the system. At this time, principal vendors should also be notified and a representative requested on site immediately. Periodic reports should be provided to the EMT on the progress of the recovery because, if the software-related disaster is long enough or severe enough to affect operations, activation of a Corporate-wide Recovery Plan

or Disaster Recovery Center may be in order. A software-related failure in a critical system may not necessitate activation of the entire Telecommunications Recovery Team, as other items, such as cleanup activities, may not be necessary. However, these members should be kept on alert throughout the procedure, both from an advisory standpoint and in case they are needed.

Major Cable or Fiber Cut

The Telecommunications Recovery Plan should also include procedures for dealing with a major cable or fiber-optic cut. The plan should not necessarily include procedures for dealing with minor cable cuts, as these are basically everyday occurrences in our profession. However, major cable cuts, particularly those of major fiber-optic links connecting cities or different portions of cities, can, in and of themselves, be disastrous.

One company we worked with a few years ago had a cable cut due to a manhole filling up with water. This particular company dealt with financial clientele, banks, mortgage companies, etc., which were very sensitive to any type of outage at all. As this outage involved water in a manhole, some users were out for up to five days before the problem could be rectified.

In another incident, this time in Missouri, a group of homeless people built a fire under a bridge during the winter season to keep warm. Unfortunately, a major fiber-optic link also passed under that bridge and was destroyed by the fire. The result was an outage that lasted several days and isolated several cities in Missouri.

Human error by technical personnel performing routine maintenance is also a major contributor to cable cuts. A case in point would be the AT&T technician in New Jersey who took bolt cutters to a 1.2-gigabit fiber-optic cable and isolated New York City for most of a day.

All of these would be classified as major cable cuts and should have something documented in the plan to address their occurrence. A few steps in this regard might include contacting the vendor and determining both the location of the cable cut and the extent of the disaster. The vendor should also, by that time, be able to tell you the cause of the disaster, such as a backhoe, a mudslide, etc. Immediately escalate the problem with the vendor, as cable cuts invariably take a long time to fix.

If the cable cut affects mission-critical systems for the company, immediately notify the Telecommunications Manager or Team Leader as well as any critical users. Normal procedures for reporting on site and providing a damage assessment report to the EMT will apply because, if the cable cut is severe enough, such as due to a mudslide or other incident, it may, in fact, necessitate activating a corporate-wide plan. The Team Leader will also make the assessment as to whether he or she should activate the Telecom Recovery Team, and, if so, which members must come to work. The Team Leader will also make the assessment on which Telecommunications Recovery Plan to implement by activating any backup communication

links or load-sharing critical traffic over the remaining links that may be unaffected by the cable cut. A cable cut is a classic example of the importance of pre-planning in any Telecommunications Recovery Plan. There are many things that a company could do to insulate itself from the catastrophic outcome of many cable cuts. However, these items must all be implemented prior to the event occurring. For companies that have not taken precautions against cable cuts, the matter is pretty much one of "sit back and wait" until the telephone company, inter-exchange carrier, or other vendor responsible for the cable has repaired it.

There are many precautions companies can take in advance of a disaster to protect against cable cuts. These include, among other things, diverse routing and self-healing networks, microwave transmission, and use of competitive providers (CLECs).

Risks with T1 Service Utilizing Proprietary Multiplexers or Routers

Another item to address in the Recovery Plan would be failure of a major T1 node. Because most major companies now utilize T1 for transmission of both voice and data services, the T1 multiplexer or router itself creates another single point of failure, often in the company's network. Similarly, companies have evolved, over the years, from using a standard garden-variety D-4 channel bank T1, for which the equipment is available literally on eBay, to advanced T1 equipment utilizing vendor proprietary solutions. This equipment is often very difficult to recover during a disaster because of its custom configuration. Similarly, if a vendor-specific multiplexer or router is used as part of the telecommunications network, a similarly configured multiplexer or router usually must also be installed at any Disaster Recovery Center in order to de-multiplex the same network traffic, particularly private line circuits.

Roll-in replacements or vendor-sponsored Recovery Plans take on an entirely new meaning in terms of T1 equipment because of the sometimes-scarcity of the equipment. These multiplexers are also increasingly software driven, which opens new doors to vulnerability in terms of software glitches or even potentially "hack attacks" through maintenance ports. They also partition T1 circuits into what a telephone company would consider oddball sizes; 128-KB or 512-KB, or 1024-KB circuits have long been part of the domain of the Data Communication Manager by utilizing proprietary T1 solutions. However, these may be completely foreign to telephone companies, which may not offer these speeds. This means that absent the recovery of the T1 facility itself, the Telecommunications Manager or DataComm Manager, in this case, is basically on his or her own, recovering the rest of this T1 node.

T1s also carry a variety of traffic, including voice communications, data communications, videos, and other types of transmissions, particularly if IP enabled.

Anyone with service running on the affected T1 should also be notified of the disaster from an advisory standpoint. LAN Managers would be included in this because, probably, critical router links transverse the T1 as well. A mirror image of both the software as well as all of the "call" or circuit designators defined in the software for the T1 mux should be copied to tape and safely stored off site. This will help greatly in the event of a disaster because it would be possible to fall back to a backup copy of the software should a software glitch arise.

A lot of beautiful solutions are also possible, however, for disaster recovery using modern T1 muxes. For example, I already explained that, for a company utilizing a Disaster Recovery Center, a similarly configured T1 mux must be stored at that center at all times because replacement of this equipment could be difficult to accomplish in a timely fashion after a disaster. If this equipment is connected using reserve or on-demand T1s, they can not only be activated quickly after a disaster but have the ability to "learn" the configuration of other multiplexers in the network in a dynamic on-line fashion. This greatly simplifies the recovery process.

Although using vendor proprietary equipment creates a new area of exposure for the Telecommunications Manager, it also makes for some very elegant solutions, as some vendor proprietary solutions can restore literally hundreds of circuits to a Recovery Center over a single 1.536-MB T1 circuit. The cost of duplicate equipment at the Recovery Center can be more than made up in reduced circuit costs by being able to move huge quantities of circuits to a Recovery Center in a timely fashion.

The Recovery Procedures for a major T1 node should also include all of the other procedures that we spoke about for other technical systems. This comprises trying to determine the cause, extent, and the nature of the disaster, as well as securing the installation from theft and implementing notification procedures for other team members and the EMT.

Other items to include in telecommunications recovery procedures include the following.

Emergency Call Lists

An emergency call list of management and recovery teams should be imported from sources that are known to maintain accurate and periodically updated files. These lists should include home and business telephone numbers, pager numbers, and an alternate means of contacting these personnel should telecommunications services not be available. This would contain, as an example, the street address for their home. As confidentiality might be a problem in these matters, it might be a good idea to use a "pointer" in this appendix to another database that is kept in a confidential location. This would keep home telephone numbers and addresses for key people from being circulated within the organization, if this were undesirable.

As we stated earlier in the book, places to look for these materials would be Human Resources, the company telephone directory, or other locations where they are subject to periodic update.

Vendor Callout and Escalation Lists

Vendor callout and escalation lists probably exist somewhere within the organization, as major circuit vendors such as AT&T, Verizon, MCI, Sprint, and the Bell operating companies all have pretty well-defined escalation procedures in cases of trouble reports. These are usually laid out in terms of first-level, second-level, and third-level management before getting into the division-level management and vice-presidents.

Your vendor should be able to provide you with an accurate escalation list up to the level of president of the vendor's company. My recommendation on this would be to put this monkey on your vendor's back! Task your vendor with the responsibility of providing you with an updated escalation list on a monthly basis or when such information changes. Then, test it periodically during your monthly and quarterly checks to ensure that it is up to date. This may not be interpreted necessarily as a negative to your vendor. By including your vendor in your disaster recovery process, you are reaffirming the vendor–customer relationship and sending a message that you intend to stay with them, as they are a part of your plan. If presented in this spirit, your vendor will probably be more than happy to help you keep your plan up to date by providing these materials on a regular basis.

Forms Associated with the Plan

It's probably a pretty good idea to have the various forms associated with keeping the plan up to date stored within the plan itself. One popular type of form to use is a two-part form. The top of the form has the name, address, telephone number, and personal information of the primary Recovery Plan member, and the bottom of the form has the same information for any replacement for that person should the primary person change positions. The form is designed to be folded in half, stapled (for security), and submitted to the person responsible for the maintenance of the plan by the Human Resources Department or other organization involved in the employee changing jobs. You may also want to design various forms for changes in equipment, software configurations, revision numbers, etc. Bottom-line, employees will eventually become accustomed to going to Section Three for dealing with inventory and report forms of all types.

Hardware and Software Inventories

This section would include an itemized listing of hardware and serial numbers to aid in rapid replacement of the equipment in a disaster. Helpful data would include the date the equipment was purchased, purchase price, as well as who it was purchased from and under what terms. Also, how long an amortization schedule the equipment is on, and other items that could aid in replacing the equipment quickly or making fast command decisions on whether to scrap the equipment and buy new or attempt to have it restored by a restoration company are also helpful information.

Similarly, Section Five would include software lists and license numbers, as well as name and contact numbers for these vendors, to replace critical software for your systems.

Team Member Duties and Responsibilities

You will need to designate a Team Leader and team members. It will be the responsibility of the Team Leader to outline a series of duties and responsibilities of team members for use in a disaster. Senior management will approve these. There could be off-site storage teams or people responsible for going and picking up magnetic and printed media from off-site storage locations. They might also include logistical teams for putting together administrative support for persons in a disaster as well as voice communications recovery persons responsible for command-routing 800 service, remote call-forwarding, local telephone numbers, and providing command and control to the EMT as well as other coordinators of the disaster. It would define persons responsible for data communications, restoring critical router links, T1 service, and other types of services. It may also define people responsible for damage assessments in other portions of the plant.

Network Schematic Diagrams and Layouts

Remember, we said earlier that the Recovery Plan should be compiled in a fashion such that any reasonably competent technical person could pick it up and ascertain what the installation once looked like, and how it should look in its emergency configuration. This is done in case persons directly responsible for recovery are unavailable or injured during the disaster. It means lots of pictures and flowcharts. Although supporting text is required, there's nothing quite like a schematic diagram picture or flowchart to quickly get the mission across to a person unfamiliar with it. These can be compiled using a number of different drawing programs that you may already have on site.

Equipment Room Floor Grid Diagrams

Associated with this material would be Section Eight, namely, Equipment Room Floor Grid Diagrams. This is important, again, when you may be recovering in a somewhat limited space, to maintain proper clearances and air flow between equipment. It should also serve as a before-and-after picture of the equipment installation to aid persons who may or may not be familiar with your organization.

Contracts and Maintenance Agreements

Your procedures should include contracts and maintenance agreements. All agreements for roll-in replacement of equipment, replacement of major components, hot-site contracts, or any number of items of this sort should be contained in this section. Without documenting them, it becomes very easy for employees to change jobs and for their successors not to realize that a roll-in replacement for a critical piece of equipment already exists. Absent this information, the company may go out and actually purchase a maintenance contract again, squandering resources, or someone's hard-fought for Disaster Recovery Plan may go completely unnoticed due to the new employee's lack of knowledge that it even exists.

Instructions for Sensitive Equipment

This section is optional but useful. Consider including special operating instructions for sensitive equipment. For example, if equipment should be shut down in an emergency, there may be instructions here for shutting the equipment down gracefully, or preserving databases, which may be in midstream. There may also be procedures to take a last-minute backup of critical equipment, if time permits, prior to shutting it down to aid in its easy restoration after the event is over.

Wireless Telephone Agreements

This is a very important section because wireless phones will play a major role in command and control in any telecommunications disaster. Every management employee within the company who has a role in the recovery process should be identified, along with his or her wireless phone number and equipment. You may also want to annotate whether the equipment is a car-mounted unit or a portable unit that could be brought into the building.

Let me alert you to a couple of precautions! Although we covered wireless in a fair measure of detail elsewhere in this text, we would like to remind you of a few things now. First, wireless is not an unlimited resource with only a limited number of send-and-receive frequencies per carrier serving your immediate area. It

could become very easy to saturate these resources in the event many companies are out of business at once, as in a central office failure. Secondly, your listing should also include a policy for employees, stating which employees are not authorized to use their cellular phones in the vicinity of the company when a disaster has been declared. Again, as there are only a limited number of send-and-receive frequencies per cell site, it is more important to conserve these frequencies for critical recovery applications than to have employees casually driving by, describing the scene to others and tying up these critical frequencies in the process.

Other Tips

A few final, helpful hints regarding the Recovery Plan will be in order. We usually recommend that three copies of the Telecommunications Recovery Plan be produced. The first plan is to be stored with you on site; the second, to be stored at home; and the third to be put in the trunk of your car. This pretty much covers any contingency. However, a minimum of two copies should be produced, and one always stored at home. One good test to try on your employees is to have a staff meeting and announce that the company has just had a disaster, and what your employees have in front of them is what they have to recover with, and then escort them from the building. Although this would be disruptive on a workday, it does drive home the point that if the employees have not stored that plan off site, they won't know what to do. Anyone caught that way one time usually remembers subsequently to store his or her plan off site.

This is why several walk-throughs of the planning document are so important. Employees who have subsequently let their Recovery Plan become outdated will have the point very forcefully driven home to them when they try to implement the Plan.

Summary

To summarize, remember the basic objectives of codifying a Recovery Plan. First, it is our belief that people involved in providing technical services to companies on a day-to-day basis are more than capable of recovering the company in a disaster. After all, in most cases, these people often built the very system in trouble and have committed to memory the vendor telephone numbers and persons who can help in a disaster. The problem occurs when they are unavailable or incapacitated by a disaster. This is why the Plan should be written at a level of detail to allow any reasonably technically competent person to execute it in the event the primary people are unavailable.

Secondly, the plan must be able to dovetail into the Corporatewide Recovery Plan, both to avoid duplication of resources and to allow for a seamless recovery solution between departments. Use pointers.

Thirdly, provision must be made for testing, training, and maintaining the Plan. These should be codified in the Corporate Telecommunications Standards Document.

Finally, multiple copies of the Plan should be produced and stored off site to assure that a copy is available when needed, regardless of circumstances.

CHEAP THINGS YOU CAN DO TODAY TO MAINTAIN COMMAND AND CONTROL

- Remote access to call forwarding
- Command routing
- Foreign exchange (FX) service
- VOIP phones

Also Consider:

- Wireless
- Two-way radio

OTHER CONSIDERATIONS

- Low power broadcast station
- Text messaging/paging/blackberrys
- "Outside" e-mail and Web hosting
- Instant messaging services
- Conference bridges

About the only thing regarding the future of telecommunications and the future of Telecommunications Disaster Recovery is that these technologies will continue to outpace our ability as technologists to back them up. As such, we should always be in a proactive mode as we become more and more dependent on these systems. To assure that the interest of our organization is well served, our primary consideration should be that no technical system be installed, no matter how much more convenient it makes doing business, especially if it adds to the exposure of the company or creates the possibility of a catastrophic disruption.

Nonetheless, if the past is any indicator, as more and more dependency becomes apparent in the telecommunications environment, more and more services will become available to address these concerns. This makes our jobs as technologists all the more important because we must evaluate all of these numerous and ever-increasing options and chart a safe course for the company to take, as a whole. It is my sincere hope that the tactics and techniques outlined in this book will help you not only with your present environment but also looking forward to the future as we accept this challenge and move into the exciting technological world of tomorrow.

Recovering Emerging Technologies (Frame Relay, VoIP, ATM and More)

BONUS!
This section contains explanations of telecommunications equipment and related technologies for non-telecommunications professionals.

If you've ever asked "What *is* this Stuff?!" (maybe you are an auditor, or would just like to know what you are paying for!), this section is just for you. (See Figure 7.10.)

What Is a Mainframe?

Mainframes do a couple of things really well. They are the cheapest way to deploy lots of computer (CPU) cycles to a large number of users. Mainframes are also good for applications that encompass repetitious tasks, which are easily automated. Examples include airline ticket sales, rental car sales, and just about any kind of business where customers call in or walk in, and where an agent fills in fields to sell a service. Insurance policies are another good example. Everyone fills in the same information, name, date of birth, address, etc. If your business is characterized by any of these processes, mainframes are probably the ticket. The nice thing about mainframes is that there are no less than 25 years' worth of standards for backup and recovery of these devices. Sungard, IBM Recovery Services, and a host of other providers provide a wealth of experience for mainframe backup. As mainframes are the oldest components in the network, it stands to reason they are, generally speaking, the most advanced recoverywise.

What Is a Front-End Processor?

You can imagine that a mainframe supporting hundreds of telemarketers, for example, is probably a pretty busy box. Therefore, mainframe manufacturers invented a "traffic cop" to direct all the messages from the users into and out of the mainframe to avoid bogging it down. The front-end processor, therefore, is just as the name implies. It's a gatekeeper to the mainframe. Typically today, this box is gone, having been replaced by a big LAN switch or router. And, indeed, many of these devices are overtaking and ousting the front end owing to their flexibility and ease of integration into distributed LAN networks. For this reason, the front end is an endangered species. When you look into your crystal ball, ten years from now you will still see a mainframe. These computers are just too good at what they do and very inexpensive for a large organization to dispense with them. Front ends, however, don't seem to be on the radar.

By the way, a common name for both of these boxes is the legacy network. Legacy, as the name implies, means the "holdover" technology from a bygone era,

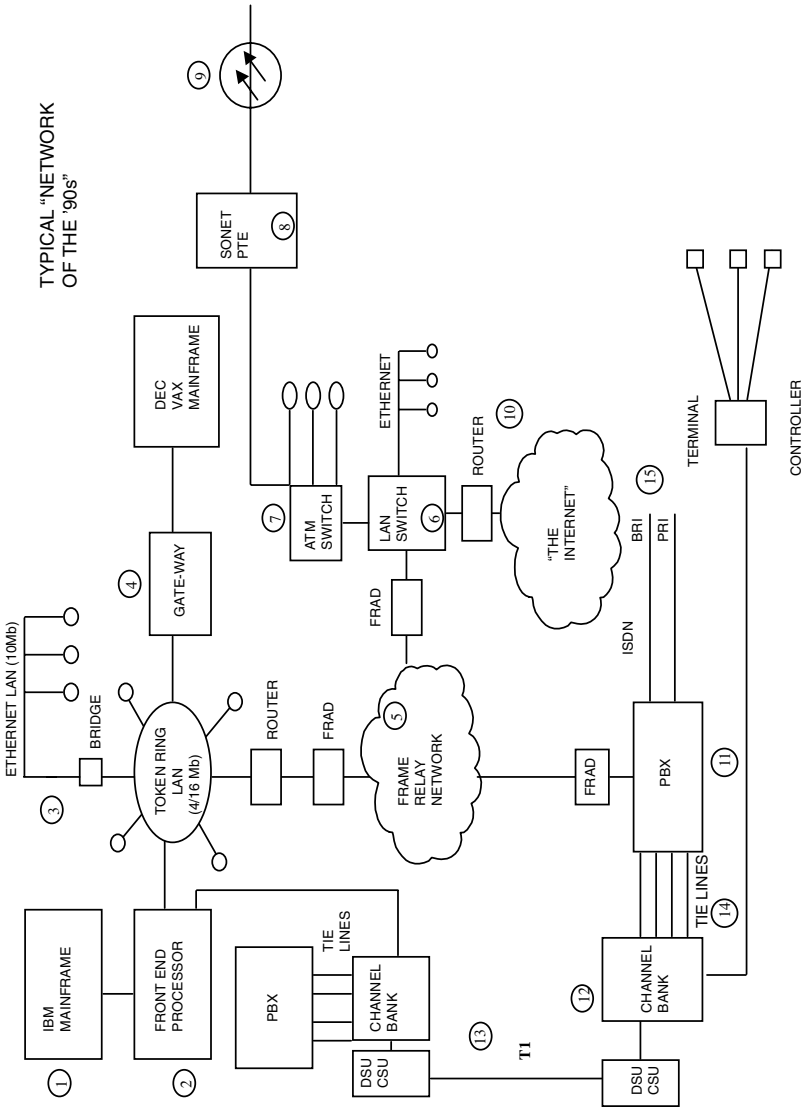


Figure 7.10 Typical "complex" telecommunications network. (From *The MIS and LAN Managers Guide to Advanced Telecommunications Planning*. IEEE Books, ©1999. With permission.)

and is loosely interpreted to mean the mainframe environment. So, what is replacing the legacy network? It's the LAN network. LANs present special problems for the recovery planner.

What Are LANs and Open Systems?

Open Systems are characterized by the following:

They are local, meaning within a building or at most a campus environment.

You own them, not the telephone company. That means the bits are "free" once the initial investment has been made. It also means that, in case of trouble, you are on your own. LANs usually run on copper. Older technologies used coaxial cable, whereas most new ones use unshielded twisted pair (UTP) rated for the particular speed of the LAN.

The most prevalent LAN technology out there today is Ethernet. Ethernet was originally designed to run at 10 Mbs but has been all but replaced in large organizations by Fast Ethernet, or Gigabit Ethernet, which operates at 100 Mbs + and is sometimes called "GIG-E." This has chiefly been the result of a major drop in the price of Fast Ethernet cards and the greater bandwidth (capacity) demands of the user.

What Is a Bridge, Router, or Gateway?

In much the same way as a front-end processor is the gatekeeper to the legacy environment, a bridge, router, or gateway is the gatekeeper to the LAN environment. With the front-end processors going away however, these components take on new importance to the recovery planner. First, are they LAN components or wide area network (WAN) components? The distinction is hazy.

Bridges basically isolate and filter different LANs from one another. This way, if one LAN segment gets really busy, it doesn't slow down the whole organization. On the other hand, if the two segments need to communicate with one another, the bridge will forward a message to the other segment. That's why people commonly describe the function of a bridge as two things: filter and forward.

Routers and gateways act similarly but have a few more brains to them. For example, bridges are not particularly good at dealing with ambiguity. If more than one path exists to a user (common, as networks are often engineered to provide multiple paths for fault protection), a bridge is not particularly well suited to selecting the best one. A router or gateway, on the other hand, is much more capable in this area.

What Is Frame Relay?

As we stated earlier, frame relay is still a popular technology that has replaced most dedicated circuits or "private lines." In our diagram we have it illustrated as a "cloud." I hate clouds. My first question to a vendor is what kind of network is inside the cloud? That's the part the contingency planner needs to be concerned about. Frame relay networks, and indeed any kind of packet technology, does fail. It therefore requires an understanding of what is inside the cloud in order to assess the risks.

So why is frame relay useful? In a word — economics. For example, imagine for a moment that I was a competitive postal provider and offered you this deal. I'll deliver a letter anywhere in the United States for five cents. Sound interesting? Good, I'll go on.

In order to get this rate, you have to follow some rules. First, you will have to commit to some minimum volume of letters you will let me deliver. Secondly, you will need to use MY envelopes. Don't worry, I'll provide you the envelopes. Thirdly, you can put no more than one sheet of paper per envelope. If you want to send a three-page letter, you must use three envelopes. Even so, that's still only 15 cents, less than half of what the post office charges. On 100-page documents from the legal department, you can always drop it in priority mail using your old postal carrier.

In keeping with this analogy, consider the following. If you mail five letters to Dallas on the way to work in the morning, then five more at lunchtime, then five more at 5 P.M. on the way home:

1. Will all 15 letters arrive in Dallas at the same time?
2. Will all 15 letters get to Dallas in the same way?
3. Will all 15 letters even get to Dallas on the same DAY?
4. Are there any guarantees that all 15 letters will even get to Dallas at all?

The answers to 1, 2, 3, and 4 above are all "no." The same holds true for frame relay.

First, 15 data packets sent on a frame relay network to Dallas will not necessarily get to Dallas at the same time. That's because not all 15 will take the same path through the network. The carrier decides that, based on network conditions at the instant you send the data. Just as you may take a train, aircraft, or truck, depending on the time you send it, your data similarly will take different paths. This is what happens inside that cloud.

There is also no guarantee that the data will get there at all. If the frame relay network gets too busy, a few packets might be thrown overboard. However, when you think about it, even with a dedicated circuit, there is no guarantee that your data will get to the far end. That's why there are higher-level protocols like TCP/IP or SDLC that check for lost data or packets delivered in the wrong order. That means Frame Relay works great for data and it's cheap, but what about voice or video? Video requires a continuous bit stream with the timing relationship of the

bits maintained. Another word for this is ISOCHRONOUS. That's the word I told you to remember earlier because it's important. Here's why.

For example, if I am watching the Dallas Cowboys on TV here in Dallas, and Emmitt Smith rushes for a touchdown, I get to see it about a half a second earlier than someone in New York who would be receiving their view of the game via network television satellite. We see the same play, however, and even though the New York viewer sees the play delayed by half a second (because of the propagation time to the satellite), he or she sees the same thing I do.

Imagine, however, that the video image was sent over a frame relay network, where there were no guarantees that the bits would arrive in order. I could just hear John Madden now:

He's at the 40!
The 30!
The 35!
The 20!
The 5!
The 10!

ISOCHRONUS VERSUS NONISOCHRONOUS

When it comes to traffic that may be intolerant of delay, like voice and video, remember my Emmitt Smith example!

Get the picture? In light of this fact, would you use frame relay to back up your company's video conferencing network? Only if you didn't mind your boss looking like Emmit in the preceding example. There are frame relay services that provide nearly isochronous services, but the time to inquire about them is before you need them in an emergency, not after.

What Are LAN Switches?

For lack of better words, LAN switches are "souped"-up bridges. Not only do they filter and forward, but they have advanced network management capabilities that allow the technologist to keep an eye on the network through proactive maintenance. Moreover, LAN switches are FAST, and for that reason they often replace routers. Lastly, today's LAN switches allow myriad possibilities for mixing and matching different equipment, components, and environments for truly seamless

solutions. These are discussed further in the LAN section. Watch them in your planning efforts; they are often proprietary and difficult to replace in an emergency. Ask your vendor about roll-in replacement guarantees and who air-ships in new equipment after a disaster.

What Is ATM?

What is a user to do if he desires the economies offered by frame relay combined with isochronous capabilities for voice and video? What if a user wants to eliminate the distinction entirely between his LAN and WAN environment? What if a user needs to move multiple gigabyte diagrams such as computer-aided designs or x-ray images? What if users need a single, integrated network access for voice, data, video, image, multimedia, etc., with virtually limitless speed and flexibility? These describe the characteristics of the ATM user. As we stated earlier, if comedian Tim Allen were allowed to "rewire" frame relay, he might come up with ATM. It's happening today in companies across America, and you need to be ready to back it up.

Disaster Recovery in SONET as a Smart Media

If there is one thing we did well earlier, it was talk up SONET. SONET is replacing T1 and T3 as the backbone transmission media for enterprise customers, and for good reasons. The impact on the contingency planner is positive. As T1 and T3 are eventually going away, SONET presents the recovery planner a 30-year planning window. How often do we get a planning window that long! That's the thing about transport technologies. They have a nice long life.

A "reverse co-location" arrangement can be requested from a competitive or incumbent local carrier — and charge them rent. SONET is also far smarter than T1. T1 was originally designed as a means of combining 24 channels between Bell central offices onto four wires instead of 96. T1 was designed for VOICE. T1 is dumb. In fact, if you put a T1 and a cinderblock into an intelligence contest, it would be a tie.

SONET, on the other hand, is SMART, clean, and error free. It has the capability to repair itself if the fiber is cut through — a feature called *fault protection switching*. What an elegant feature for a business resumption planner! SONET also has nonintrusive maintenance features — meaning you don't always have to take it down to test if it has trouble, *and* SONET is designed for glass fiber optics, the mainline telecommunications medium in place today. Your users will pay for the features in SONET, and the technology is more available today than ever.

What Is Fiber Optics?

Fiber optics is the medium used for virtually all high-capacity communications services. By high capacity, this means essentially anything about the T3 rate of 44.736 Mbs. Fiber is also used in the LAN environment as a high-speed connection between LAN switches and other components. Fiber can also be used to connect mainframes together at the channel level in the legacy environment. There are two kinds of fiber:

1. Single-mode — This is what the phone companies use.
2. Multimode — This is probably what you have in your building.

What Is the Internet?

Everybody knows what the Internet is, but how did it get started? It is actually rooted in contingency planning and therefore has many useful features built right in. Imagine you are the U. S. government in the 1960s and 70s, planning for the prospect of incoming Soviet ICBMs. Intuitively, the war planners of the time knew that 20 minutes after a launch, virtually every telecommunications hub in the United States would probably be in the upper atmosphere. This presented an obvious problem.

As any potential opponent would probably hit telecom hubs first (thereby taking out the eyes and ears of its opponent), some survivability had to be planned for. The first thing the government did was build big telephone centers in relatively outlying locations. We've already discussed the example of Ennis, Texas, population 14,000, about 30 miles south of Dallas. A nice little town, good Czech sausages, and one of the biggest AT&T offices I've laid eyes on. I'm not sure if it was part of the '60s effort to harden the public network, but it sure fits the bill: uncharacteristically big for the town, no windows, and 30 miles from ground zero.

Even with precautions like these, however, it would be difficult for data communications to take place using the traditional master–slave, host-terminal environment. It would be logical to assume the host would be in a big city. That means that even with the path in place, data communications would still be out of the question.

Just what if each node in the network was just a little bit smart? Distributed intelligence with nobody in charge. (Kind of like my office.) The idea behind the Internet was that data could be put in packets with a header address to where it was destined. This packet is called a *datagram*.

After a first strike, some parts of the network might still be intact. Using a distributed intelligence topology like this one, messages might eventually get through. This was the beginning of the Internet we know today.

Routers are just a little bit smart. They are better at dealing with ambiguity than bridges. For example, they can select an "alternate" path when the usual one is out, based on internal lists called *forwarding tables*. Routers, like everything else, require special software called TCP/IP. Routers don't care what the data is. They just route datagrams to the next router available.

When you access a Web server today, this "bucket brigade" system of distributed intelligence routes datagrams to and from their destination. Only, today the government is out of the picture, the Web is commercially supported, and nobody owns it. That's the problem. The Internet is rooted in contingency planning and in fact was designed as a Department of Defense system. The only problem is: because nobody owns it, who controls it? The very thing that makes it survivable also makes it unpredictable.

As the Internet is, in fact, a collection of servers, "distributed intelligence with nobody in charge," it is difficult to control. This will be a policy decision that must be taken up by management. Can a company put mission-critical data on a network that nobody controls, and where there is no quality of service guarantees? The industry has answered: YES. On the other hand, the World Wide Web has more users today after just ten years than the telephone network had after 50. It is clearly positioned to be revolutionary.

What Is Voice Today?

Much of what we have covered so far has been data oriented. PBXs are for voice. PBX stands for *private branch exchange*. It's a private telephone switch owned and maintained by your organization, on its own premises. It is also probably a misstatement to say that PBXs are only for voice. Some of them also do data, video, etc. Not surprising, however. In today's networks, voice is really data. So is data. Any questions? Relax, the statement is true.

What Are Channel Banks?

They are still out there, that is what they are, even though pulse code modulation (PCM) is 1940s technology. Again, they are transport technology, so they hang around forever and work like a horse. Channel banks take a T1 (described in the following text) and break it into twenty-four 64-Kbs voice channels. This was what T1s were originally designed for. A T1 was a cost-effective means of taking 24 interswitch trunks between Bell or AT&T central offices, and combining them onto a four-wire copper circuit. As the technology worked so well, and because it's been out there for so many years, it has found its way to the end user as well. Today, virtually all medium-sized end users utilize T1 access lines to combine dial tone lines, trunk lines, and other voice and data services.

What Is T1?

Think of a T1 as a 1.536 Mbs *data circuit* designed for voice. If you take twenty-four 64-Kbs channels and multiply the numbers together, you get 1.536 Mbs. Add

8 K more that the phone company uses to tell them all where to line up and you get 1.544 Mbs. That's the T1 speed. You can think of a T1, in fact, as a 1.544 Mbs data circuit. Twenty-four circuits share this circuit, and each one gets exactly 1/24 of the capacity. T1 is unquestionably the most widely deployed transport technology today and one that must be evaluated thoroughly by the recovery planner.

What Are "Private Lines"?

Pretty much going away, that's what, except for specific applications. Increasingly, frame relay or VoIP have replaced private lines, but there are still a lot of them out there. They must also be taken into account in any business resumption plan.

There are over 200 different kinds of private line circuits. These range from "hoot and holler" lines to digital data circuits. A hoot-and-holler line is pretty simple; in fact, it is just a pipe. It doesn't even ring. The user just picks it up and yells (hence the name): "I want to trade 100 shares of AT&T at 52!" or "I need a fender for a 1964 Chevy!" Junkyards and stockbrokers often use this kind of circuit. If you are a brokerage company, you probably have hoot-and-holler circuits. The correlation of the junkyard and brokerage company is purely coincidental (or perhaps Freudian?). If these are still in your organization, they present challenges to backing them up.

What Are ISDN and xDSL?

ISDN was designed way back when to replace POTS (remember that's "plain ordinary telephone service") by bringing digital to the doorstep of the small-office-home-office (SOHO) user. The copper cable that serves the typical small office or residence is really capable of carrying more than just a single voice call. ISDN BRI (basic rate interface) takes advantage of this by providing two 64 Kbs channels on the same two wires that previously carried POTS. In fact, it looks and acts like a miniature two-channel T1. The common name is 2B+D. That means two bearer channels with one delta channel. The "B" channels carry the actual information. The "D" channel can be thought of as the "supervisor" that instructs the two "worker Bs" what to do, how, and when.

ISDN also comes in a jumbo economy size. Primary Rate Interface or PRI can be termed "T1 Deluxe." It looks, acts, and quacks much like a T1 but has some additional features. It has 23 channels that carry either voice or data traffic, plus a 24th channel (a supervisor) that controls the whole show and tells the rest what they are and what to do. The common phrase is 23B+D, or 23 bearer channels with one delta channel. Lots of companies still use BRIs! Look for them in your network. For your convenience in remembering which is which, just think BRI and PRI. B is for baby, P is for Papa. PRI is used primarily for PBX access just like a smart T1. BRI, however, is surging in use as a means of surfing the Internet at 64 or 128 Kbs.

xDSL works on the same principle. It runs an analog signal over standard 19–26-gauge copper wire to create a high-speed data path, while at the same time carrying voice. It is the technology of choice for many telecommuters and small businesses. (See Figure 7.11.)
* NOTICE THE "NETWORK" GOT SMARTER? RATHER THAN JUST "DUMB" LAYER 1 TRANSPORT. THE "NETWORK" TODAY DOES LOTS OF OTHER THINGS! This is useful for disaster recovery!

What Are Smart Networks?

With the profound advances in everything else electronic, it is no surprise that the network has gotten much smarter as well. In fact, in my earlier days as a private line board technician, networks were downright simple. All I had to say was "I got tone" (meaning there was continuity on the line) and then — this was the good part — it was somebody else's problem! That's not the case today. Networks — like the telco's networks — do lots of other things. And yes, there are important ramifications to the contingency planner.

The OSI reference model is shown in Figure 7.11. T1 lives in layer 1 — the physical layer. Ethernet and Token ring live in layer 2. TCP/IP live in layer 3 and 4. The application lives in layer 7. The TCP/IP model on the right is simpler and shows only four layers: the application layer, TCP layer, IP layer, and network access layer. Gee, I like the TCP/IP model better.

Notice the network layer got bigger? What used to be just a dumb, one-network layer in the OSI model now goes to layer 2½. This is because networks have gotten smarter. Frame relay, for example, does routing, switching, segmenting, error

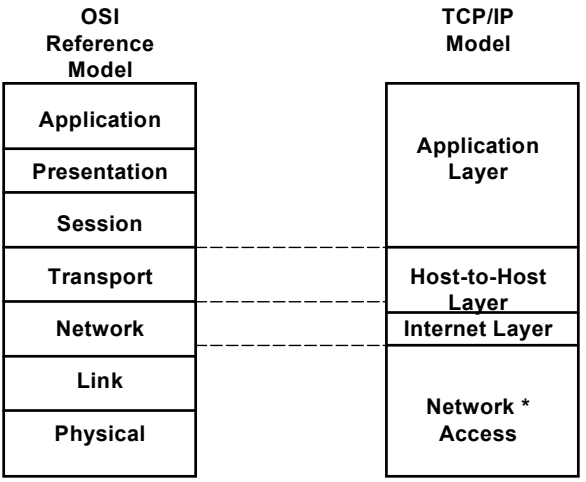


Figure 7.11 The evolution of "smart" networks.

control, and other higher-level functions that used to be IS rather than telecommunications functions. We'll discuss the implications of these smarter networks later as well.

The "legacy" version of data transfer is shown in Figure 7.12. Mainframes and front ends used SDLC, and the applicable components are highlighted for your review. A logical diagram also shows the "envelope in an envelope" example in a comparison of IP and the post office.

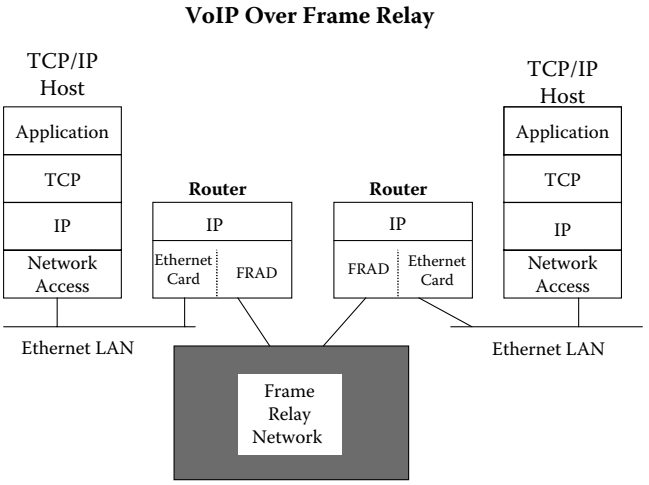


Figure 7.12 Today's smarter networks: a two-edged sword when it comes to disaster recovery.

CHAPTER 7
WORKSHEETS

WORKSHEET No. 1

Incoming 800 Service

Priority and Redirection Form

Call AT&T at _____ to implement redirection of these numbers. For further information, see Appendix ___ .

Number	*Department*	*Use*	*Priority*	*Emergency Number*
(800) 725-6870	Customer service	Main #	H	(214) 733-6870

WORKSHEET No. 2

Incoming Telephone Service

Priority and Restoration Form

Call Verizon at _____ to implement call forwarding of these numbers. For further information, see Appendix ___.

Number	*Department*	*Use*	*Priority*	*Emergency Number*
(800) 733-6870	Customer service	Main #	H	(602) 759-7502

WORKSHEET No. 3

Private Line Service

Priority and Redirection Form

Circuit Number	*Department*	*Use*	*Original Destination*	*Emergency Destination*	*Priority*
(800) 725-6870	**Customer service**	**Main #**	**H**	**(214) 733-6870**	

WORKSHEET No. 4

Long Haul Carrier Checklist

(FIBER-OPTIC-BASED CARRIER)

The following make good discussion topics for your long-distance carrier.

1. Does your company employ fault-tolerant ring topology? _____
2. Is our company on a ring? _____
3. Is the ring LIT? (Electronics installed.) _____
4. Will your company redirect our service in the event of an accidental fiber cut? _____
5. If so, will you redirect switched service only, or private line service as well?
6. Will such a transfer be a manual patch or automatic? _____
7. Will we experience network blockage when this happens?_____
8. If so, how much (in percent of normal capacity)?_____
9. Can you, as a carrier, suggest any improvements that can help us? _____

Author's Note: In 1993, it was predicted that fiber-optic rings would be virtually ubiquitous by now. Not so. Although many companies have made the investment, many — even large ones — have not. Therefore, checklists like these are more valid than ever. Use them!

WORKSHEET No. 5

Local Access Carrier Checklist

The following makes good discussion topics for your local carrier.

1. Does your company employ fault-tolerant ring technology? _____
2. Is our facility on a fiber ring? _____
3. If we are not served by fiber, can it be economically provided to us? _____
4. Where is the next nearest CO? Can we get a second path to it? _____
5. Exactly where do our present facilities run (by street, side of street, etc.)? ___
6. Is this area prone to frequent digging or construction? _____
7. Can you, as a carrier, suggest any improvements that can help us? _____

Note: Often providing fiber where none exists can be an expensive proposition. Nonetheless, we have seen many instances where carriers have provided it free to companies expecting significant growth. It's more convenient for the carrier. If you are expecting such growth, make the carrier aware and be sure to request a fault-tolerant ring if the carrier desires to install fiber.

WORKSHEET No. 6

Software and Traffic Management Disruptions

1. Do your users report frequent "all circuits are busy now" recordings on local calls? _____

2. Do your users report frequent "all circuits are busy now" recordings on long distance calls? _____

3. Do your callers report experiencing frequent fast busy signals? _____

4. Do you ever experience problems calling specific prefixes or area codes? ____

Chapter 8

Notification, Teams, Recruitment, and Testing

Leo A. Wrobel

Contents

How Do You Start? 241
Evaluating the Results of a Disaster Recovery Test 257

How Do You Start?

Sounding the Alarm

Notification and response procedures for various types of disasters can be a complicated proposition. As pointed out earlier in this book, there are several different types of disaster responses that may be called for, depending on the situation.

For example, if a major piece of equipment fails, you would presumably be the principal respondent team responsible for its restoration. Conversely, if the entire building is gone, you will essentially be in a "supporting-cast function," taking your direction from the EMT (Executive Management Team) and coordinating with other teams. This makes it important that your particular team is notified in a timely fashion in cases of major equipment loss. It is equally important that the determination of the type of disaster and level of involvement is made early on in the process in case the response must be broader in scope. We will begin by discussing how this happens.

The following diagram is intended as an example of a particular department, in this case, the telecommunications function. It illustrates a logical sequence of events in a timeline fashion. It may be useful in getting your thoughts in order and

for considering the flow of your processes in the opening hours after a disaster (see Figure 8.1).

Who Should Be Included in Notification of a Major Disaster

- Executive
- Legal
- Finance
- Audit
- Marketing
- Sales
- Operations
- Technical services
- MIS
- Telecommunications
- Facilities
- Security
- HR
- Others

In the figure, the first item on the timeline is the **notification**. It is important to consider that the notification may not come from anyone in your chain of command. More likely, the notification will come from someone such as a security guard, facilities manager, or perhaps even the fire department. Carefully consider how your information flows during this early notification phase. For example, if a security guard is making his rounds late at night and discovers the air conditioning to a major equipment room has failed, will he or she know enough to notify you directly, or will the problem be treated strictly as a facilities failure? Needless to say, loss of air conditioning is a serious matter in a room full of expensive (and heat-producing) equipment.

When pondering all of the various things that can go wrong within a building, also be sure to consider who would be the first to notice something wrong should a given event occur. Most building security organizations, for example, keep some type of a log or callout book. Even if these employees are rented or outsourced, they will undoubtedly report to someone upstream, internal to the organization. They also probably have a book or written procedure that tells them who to call should something unusual happen after hours. Be sure that you are a part of this procedure and that they know to call you at the first hint of trouble.

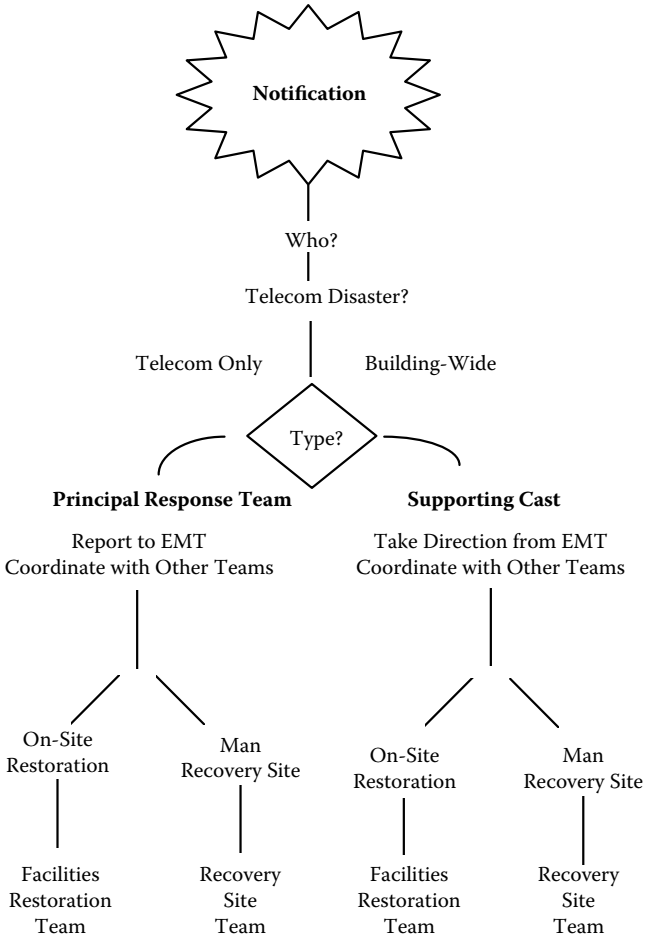


Figure 8.1 Example of notification procedures.

After you are satisfied that you will be properly notified after a serious event, you should turn your attention to the events that must occur after you arrive on site. Consider the checklists in the following pages.

Once you have been notified and arrive on the scene, it will be necessary to make a quick determination as to whether the damage is buildingwide and thus involves multiple departments, or whether the damage is confined to equipment alone (see Figure 8.2).

The procedures you implement will be based in large part on this initial assessment. For example, if the damage is confined only to equipment, if a power supply goes out in a router or multiplexer, the damage certainly affects the company as a whole, but the response is coordinated principally by the Technical Support rather than the Corporate Response Team.

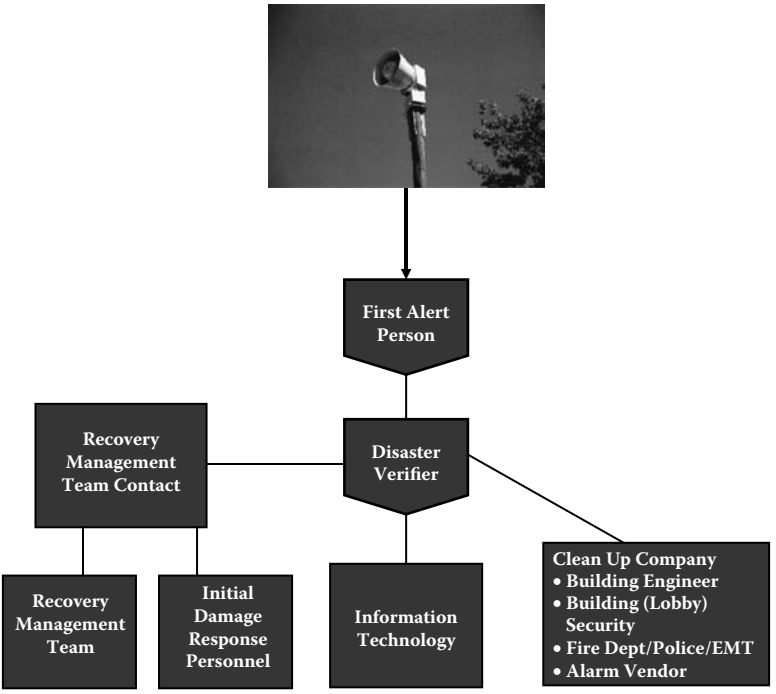


Figure 8.2 Example of "first alert" procedures.

In this case, the Technical Support Response Team will keep the EMT or other corporate entity apprised of the status of the recovery but will be basically acting on its own to rectify it as the team is confined only to its area of responsibility. This team will also be expected to coordinate with other teams as necessary. For example, the Facilities Group would be consulted in matters of power or common facilities.

If, on the other hand, the disaster is more global in nature, such as something affecting the building (fire, water, etc.), the Technical Support (MIS, Telecommunications, etc.) Team will actually be acting in the role of a "supporting cast," taking its direction directly from the EMT. The team will still need to coordinate with the EMT, but may be called to perform tasks that are perhaps outside the auspices of Telecommunications. This is principally due to the fact that, in a companywide disaster, there are several things to be concerned about other than equipment.

TECHNICAL SERVICES RECOVERY PLAN

(What to do first after you arrive on site)

Fax this form and the following one to the company's EMT at (____) ____-_____ within 90 minutes of your arrival on site.

Location_____

Time of disruption _____

Nature of disruption _____

Extent of damage_____

_____

_____

Injuries_____

Present status _____

_____

_____

Time of next report _____

Equipment Damage Report

Fax this form along with your initial notification to _____ (site cleanup company) at (____) ____-_____ and the EMT at (____) ____-_____:

Nature of damage:

[ ] fire

[ ] smoke

[ ] water

[ ] contamination

[ ] sabotage

[ ] software

[ ] power surge

[ ] lightning

[ ] other _____

Type of restoration required:

[ ] magnetic media

[ ] document

[ ] equipment — PBX

[ ] equipment — multiplexer

[ ] equipment — ACD

[ ] equipment — power

[ ] equipment — other _____

[ ] equipment — other _____

Software Response Team Duties and Responsibilities

Activities:

1. Provide a representative at recovery headquarters.
2. Specify filenames of media to be picked up by MIS at the off-site storage facility.
3. Make duplicate copies of software upon delivery, and return original to storage.
4. Verify software and hardware configurations.
5. Notify vendor to assure software releases are compatible with new equipment installation.
6. Request software patches, if available, if software hardware incompatibilities are possible.
7. Request an on-site vendor representative if required.
8. Make all remote loads of software.
9. Review software installation for correctness.
10. Test final configuration.
11. Place new configuration in service.

Telecommunications Team Duties and Responsibilities

Activities:

- Provide a representative at the EMT Headquarters.
- Provide immediate notification to all communications carriers.
- Coordinate telephone company's input to the damage assessment status reports.
- Coordinate equipment installation at the recovery sites.
- Coordinate repair or replacement of any damaged communication facilities.
- Coordinate the establishment of voice communications with the telephone company (Command and Control).

Human Resources Team Duties and Responsibilities

Activities:

- Provide a representative at the EMT headquarters.
- Notify families of injured personnel; explain benefits program.
- Obtain temporary personnel during the recovery operation.

- Provide special consideration to employees who were required to work during recovery versus those who were required to stay home.
- Provide guidance on pay and compensation for employees.
- Be prepared to provide list of employee home addresses if needed during the recovery operation.

Facilities Team Duties and Responsibilities

Activities:

- Provide a representative at the EMT Headquarters.
- Provide guidance to local authorities while accessing the facility as related to the existence of unique preventative measures (i.e., lexon windows, automatic locking doors, raised floors, etc.)
- Provide assessment of investigation of the cause.
- Assist in the assessment of building damage, including:
  - Architectural
    - Utilities
  - Electrical
    - Environment (HVAC)
- Manage building repairs and reconstruction activities.
- Manage disposal of damage residue.
- Obtain temporary recovery headquarters location.
- Obtain temporary work locations.

Finance Team Duties and Responsibilities

Activities:

- Provide a representative at the EMT headquarters.
- Alert appropriate corporate and company financial departments.
- Provide immediate emergency credit arrangements, petty cash, and travel advances.
- Provide communications with tax regulatory agencies (federal, state, and local).
- Assist in the investigation to account for any "lost" or destroyed negotiable items.

Risk Management Team Duties and Responsibilities

Activities:

- Provide a representative at the EMT headquarters.

- Notify the appropriate insurance companies.
- Obtain written releases.
- Obtain "proof of loss" documentation instructions (photographs).
- Obtain claims filing instructions.
- Provide guidance regarding actions to be taken during the salvage operations.
- Process all insurance claims.
- Advise recovery personnel as to the type of records and information to be retained for insurance purposes.
- Collect and record all recovery-related costs.

Internal Audit Team Duties and Responsibilities

Activities:

- Provide a representative at the EMT headquarters.
- Assist Security as required to coordinate investigations during the recovery.
- Verify that controls are in place for applications modified to meet limited resources available at the computer back-up site.
- Review recovery procedures to ensure assets control.
- Notify external auditors, if necessary.

Legal Team Duties and Responsibilities

Activities:

- Provide a representative at the EMT headquarters.
- Handle legal issues with next of kin.
- Advise recovery personnel on contractual obligations.
- Provide copies of contracts destroyed by the disaster.

Medical Team Duties and Responsibilities

Activities:

- Provide a representative at the EMT headquarters.
- Handle minor medical requests.
- Coordinate with local hospitals for additional medical requirements.
- Identify and locate injured personnel already moved to the hospital.
- Assist in obtaining proper nourishment for recovery personnel during initial stages of the recovery operation.
- To avoid exhaustion, ensure recovery team members work reasonable hours.

Administrative/Office Services Team Duties and Responsibilities

Activities:

- Provide a representative at the EMT headquarters.
- Alert the Post Office to the situation.
- Establish a Mail Services area within the Recovery Headquarters to handle mail for recovery personnel.
- Obtain office equipment, furniture, forms, and supplies, as needed.
- Issue purchase orders for all recovery requisitions.
- Coordinate with the corporate security officer.
- Provide security at the affected site.
- Provide security at all recovery operation locations.
- Coordinate with the risk management representative to get approval for the removal of any material from the damaged site.
- Establish area to accept deliveries 24 hours a day.

Public Relations Team Duties and Responsibilities

Activities:

- Provide a representative at the EMT headquarters.
- Coordinate radio and TV announcements to notify employees as to where they should report.
- Prepare official company statement to minimize adverse publicity.
- Direct and coordinate all press conferences.
- Provide, monitor, and control photographers.
- Develop recovery progress notifications for publication.

Transportation Team Duties and Responsibilities

Activities:

- Provide a representative at the EMT headquarters.
- Provide ground transportation.
- Provide courier coordination and scheduling.
- Provide air transportation.
- Obtain hotel accommodations.

To recap:

- Look carefully at your notification procedures to be sure that if something happens when you or your staff are not around, you will be properly notified.
- Look carefully at how you are notified. Be sure that you are a part of the procedures for security personnel.
- Lastly, look carefully at the type of disaster you are evaluating, whether it's confined only to a specific department or whether it's buildingwide, as this will directly affect your response in the opening hours following a disruption.

After these calls have been made, you will still be faced with splitting your staff and having them run in many different directions to respond to a global disaster. This will be discussed next.

Whether the disaster is confined only to your particular department or whether it's buildingwide, you will be faced with splitting your staff a minimum of two ways and probably more. If your company is utilizing a backup and recovery center somewhere, one contingent will have to travel to that location to staff it and put it into a usable configuration. The other half of your staff would be expected to remain on site to deal with restoration activities and putting the original site back in order so that business can move to its original location as soon as possible.

The names of these teams vary, but for our purposes, we'll call the team that remains on site to aid in restoration work the **Damaged Facilities Restoration Team,** and the team that travels to the backup facility the **Back-up/Recovery Site Team**.

The complement of personnel dispatched to the damaged site will first handle a survey of the damage and report back to the EMT. They will also coordinate with local and emergency authorities. The Damaged Facilities Restoration Team could also include members of the company's Building Service Group and representatives of the production, LAN, mainframe, telecommunications, or other divisions; it need not be solely technical services personnel. Company divisions with a particularly high interest in recovery will include those with a lot of equipment in the building, such as the MIS or telecommunications department. They will probably want to be involved and will dispatch at least one person to aid in the recovery. Other teams, such as administrative or logistical supply teams, should also be considered, as well as a media affairs representative in case the disaster is visible and the news media are present. Our response criterion in this case is similar to what we have discussed in other parts of the book, but with notable exceptions.

Some considerations include the following:

Did the correct team members meet at the damaged site? Be sure that only employees required for the recovery process assemble at the site after a disaster. Others who report simply to satisfy their curiosity may, in fact, interfere with

the recovery process or even hinder it by tying up valuable cellular telephone frequencies by calling their wives or husbands to describe the damage.

Did the team have at least two each of the following?

a. *Wireless phones or two-way-radios*. Wireless phones can be invaluable for maintaining command and control after a disaster. Be aware, however, that if the disaster covers a wide area, such as in an earthquake, tornado, hurricane, etc., there will be intense competition for wireless frequencies. Other companies will also be in trouble, and there could be delays due to limited capacity on the wireless network. Therefore, in addition to wireless phones, consider having other backup systems to maintain critical command and control and communications. Two-way radios are especially useful as well in situations in which there may be contention for wireless frequencies or simply as another way of keeping in touch. They are cheap and have up to a 12-mile range these days, so they are great for campus environments. In addition to being inexpensive, they require no licensing. It is a good idea to consider these for your recovery teams.
b. *Pagers*. These can also play a role in the disaster recovery process, especially when coupled with voicemail or another medium. For example, an employee could be paged at home after hours if it was difficult to reach him or her by other means and, after finding an available phone, call in and listen to the voice mail for directions.
c. *Instant messenger*. One large firm after the World Trade Center disaster actually kept in touch using AOL instant messenger. Although an unlikely candidate to be considered in advance, it was available and heavily used until this firm recovered.
d. *Low-power radio station*. You would be surprised, but a low-power radio station, similar to the kind that gives traffic or airport information may not be a cost-prohibitive proposition. They cost only around $15,000, including the license. They broadcast on a standard AM radio and can be heard up to ten miles away. This can be valuable in campus locations and as a means of getting emergency instructions out to many employees. In the nondisaster mode, we recommend using the station to broadcast items of interest to the employees, such as changes in benefit plans or the company's stock price. This will encourage employees to listen regularly. When the time comes to tune in for a disaster, they will know where the station is on their dial.

These are all useful technologies to keep track of people on site after a disaster and expedite the recovery process. The important point is to be innovative when considering technologies that keep your people together, acting as a cohesive unit in a disaster, and giving them every advantage.

Do employees have access to the following?

a. *A flashlight with a spare set of batteries*. Many people need to be reminded, however, when responding to a disaster on site, as part of a Facilities Restoration Team, that it is probable there will not be power. Therefore, a good flashlight with a spare set of batteries is an absolute necessity.
b. *A hard hat*. As the Damaged Facilities Restoration Team will also be expected to re-enter the building, hard hats and other safety equipment should be absolutely mandatory, notwithstanding the ethical concerns of keeping your employees safe. One must also consider what it would be like trying to recover the facility if key employees were injured or incapacitated as a result of re-entering the building. Think safety!
c. *An identifying badge or, preferably, an identifying vest*. This will help you quickly identify which person is an employee and which is a looter. When one considers the pandemonium that could ensue by having dozens, or perhaps hundreds, of people on site after a major disaster, the importance of identifying badges or vests becomes quite understandable.
d. *A copy of the recovery plan*. Each member of the team should also have a copy of the disaster recovery plan. Many times, employees like to keep these on their laptop computers, especially because they'll probably tote their laptop with them to the disaster site for access to their e-mail. Considering the fact, however, that there may not be a place to plug in a laptop and that battery life is finite, it's a good idea to have a paper copy of the plan in the trunk, just in case. If your team is depending exclusively on laptop computers, adapters allowing them to plug in to a cigarette lighter, for example, in a car should be considered.
e. *A small notebook* to annotate critical events and document important command decisions made during the recovery process. The importance of opening a critical events log — even one just in a small, inexpensive pad of paper — cannot be overstated. Members of the team will be called on to make a rapid series of command decisions in a very short time and are sure not to remember everything they have done. "Did I call the air-conditioning people?" "Did I notify the telephone company?" "Did I call the cleanup people?" "Did I notify the EMT?" Making a quick note of any command decisions made in the opening hours of the calamity will help you keep matters in order as well as aid with the review process after the disaster is over. Remember, this may all be happening at 3:00 A.M. Your mind may be foggy.
f. *At least one roll of quarters*. Pay telephones may be the only show going if a major telecommunications disaster renders other services unavailable or overwhelmed. Pay telephones are also the telephone company's first order of priority in any widespread disaster. As businesses may be closed and ATMs will undoubtedly be unavailable, have your employees ready to become a "cash society," at least with regard to telephone calls.

FACILITY RESTORATION TEAM CHECKLIST

[ ] Wireless telephone?
[ ] Two-way radio?
[ ] Pager?
[ ] Laptop computer?
[ ] Flashlight?
[ ] Spare batteries?
[ ] Hard hat?
[ ] Identifying badge or vest?
[ ] Copy of recovery plan?
[ ] Roll of quarters?
[ ] Critical events log?

g. Is a building facilities manager identified in your plan to interface with local emergency personnel? Remember that, after a fire, for example, you won't own your building until the fire department says that you do. Because they will have control of your facility, a knowledgeable building facilities manager could help interface with these local authorities and more quickly help decide, for example, when it's safe to re-enter the building.
h. Have you identified anyone to talk to the media? If the disaster was highly visible or widely broadcast on police or fire scanner facilities, it may be a good idea to have a trained media affairs representative on site when the mobile TV units roll up. We've seen recovery plans where companies attempt to train their employees on how to talk to the media. Statements include the following: "Don't wear sunglasses"; "Don't say, 'no comment'"; "Look directly into the camera"; "Don't chew gum." We find this a risky proposition at best. Employees are just not trained to talk to the media. Consider the following situation: The company has had a fire, and the television media, after hearing this over the police scanner, arrives on site. By the time they get there, the fire is out, but employees are still coming out of the building. The first employee exits the building and says, "Everything is under control. *It's not as bad as it looks*." The second employee comes out of the building and makes a similar statement. The third employee comes out of the building screaming hysterically, saying, "They're all dead in there. *We'll never open again!*" Which of these employees will be on TV tonight? Is this the message you want presented to your investors, shareholders, and other employees' families? Probably not. All the more reason to handle media inquiries skillfully through trained personnel.

i. Will your building be secure from theft and looting? It may be a good idea to have at least one security person on the facility reconstruction team to assess the situation and determine whether additional reinforcements are required for security. Be sure to predefine, in advance, who's responsible for security around the building. It's very easy for different departments to show up on site, each of them requesting security backup. In that situation, you could end up with 30 "rent-a-cops" banging into each other in an already confused situation. Coordinate this through Corporate Security, the Facilities Department, or one such responsible entity. It will also be the responsibility of the Facilities Restoration Team to man this staging area. Not everyone can be on site. Some of the employees responding to the disaster will be responsible for coordinating with vendors and carriers, following up on equipment shipments, authorizing payments, and performing other administrative functions involved in literally rebuilding your business overnight.

j. Is a prearranged staging area for recovery operations promptly established, for example, in a nearby hotel? If the building is totally inaccessible or lacks the required telecommunications, water, or sanitary facilities, it will be necessary to set up a staging area in a nearby location conducive to this type of business.

k. Are predetermined telephone numbers identified for staging area? For example, the network control number may be diverted to the recovery center for technical questions regarding mainframes or LANs. The help desk number, however, may be diverted to the staging area. These decisions should be made in advance. The important point is to be sure that numbers critical to command and control and to the recovery process do not change. It will be confusing enough in a disaster situation without people having to learn new numbers. This is also unnecessary, based on the technologies discussed earlier in this book, such as remote call forwarding and command routing.

l. Do you have provisions to notify a professional cleanup company? For that matter, do you know the best place to put magnetic tapes that have been wet in a disaster until the cleanup company arrives? Professional cleanup companies have an answer. Put them in the freezer! Many people don't realize it, but these companies employ a freeze-dry process to save valuable data stored on magnetic media. They have similar processes for paper that has been wet, or equipment that is smoke damaged. These companies should be immediately notified after any disaster because much of the magic they work on equipment, tapes, and paper must happen within the first 48 hours immediately following a disaster. After that, it's too late. Beware of the turf issues that can develop with regard to restoring a building. Although your principal focus probably revolves around the equipment and saving it, other people will have different concerns. You

may have to contend with other people in the company more interested in saving the original artwork in the lobby than they are in saving the computer room!

THERE ARE A LOT OF "R"s in Disaster Recovery Planning

1. Recognition
2. Response
3. Recovery
4. Restoration
5. Return to normal
6. Regroup
7. Reorganize
8. Rest and relax
9. Reward

m. Is there a provision to seek help from your vendors? Are all numbers on the escalation list for these vendors current? One of the simplest things to check in any activation or test is whether the telephone numbers for key vendors and carriers are up to date. If these numbers are obtained from known good sources, as discussed earlier in this book, there should be no excuse for them to be out of date. The minimum criteria for a successful test should be that the numbers are current and working.
n. Is adequate equipment for entering the building available? Remember, earlier in this chapter we spoke about items such as hard hats and flashlights, which will be necessary to enter a damaged building. What else is needed? Jot these down during the test so you will remember the next time.
o. Which department is responsible for rewiring the building? There are probably five different people in the organization who will tell you that they are responsible for wiring. This could include Facilities, LAN Management, Telecommunications, and other departments. Be sure responsible people are predefined in advance to avoid overlap, wasted efforts, and squabbles during the recovery.

Assuming your company is using, or supporting activities within, a commercial recovery center, it will also be necessary to dispatch a team to engage in these activities. Although the makeup of this team will vary, depending on the company's size and the nature of the operation to be supported, some suggested titles for those on this team include:

1. Help Desk Coordinator — This person will be responsible for establishing a staging area at the recovery center to coordinate overall recovery activities. This would include fielding inquiries from vendors, carriers, and other company locations, as well as getting messages to people engaged in recovery activities at the center. This person should have a very broad base of knowledge and also attempt to serve as a first-level trouble resolution point to avoid having to interrupt those involved in configuring the center.
2. Principal Engineer — If staffing allows, it's a good idea to have at least one principal engineer or analyst available at the center to provide second-level troubleshooting and help iron out the more difficult problems that arise during the activation. Even if these troubles do not materialize, the principal engineer/analyst can also help, as an extra pair of hands, in configuring the center promptly.
3. Vendor Liaison.
4. Carrier Liaison — Although it's possible to split duties at the recovery center a number of different ways, for the purposes of our example, we've basically divided tasks between those that are inside and those outside. The vendor liaison would handle the setup of all types of telecommunications equipment at the center, such as multiplexers, CSUs, DSUs, ISUs, etc. The carrier liaison, on the other hand, would be more concerned with everything outside, namely, optioning, configuring, troubleshooting, and testing of private lines, and dial-up and digital circuits required at the center. The carrier liaison, for example, would test T1 loops to ensure they were optioned with the right line code to support the equipment configuration being installed.

EVALUATING THE RESULTS OF A DISASTER RECOVERY TEST

By this time you should have a fair idea of what goes into a properly produced disaster recovery plan, and are well on your way to a successfully documented procedure.

Documenting your plan, however, is only the beginning. It's important that some type of measurement criteria are in place to determine its effectiveness and, for that matter, whether the plan works at all. This means learning how to test the plan.

By reviewing these before activating a recovery test and making the necessary adjustments in your recovery plan, it is hoped that you can avoid errors similar to these and make for a more cohesive and smooth-running recovery exercise.

The Executive Management Team (EMT)

For the purposes of our fictitious exercise, we are going to model a fairly large company that uses the EMT concept. As we discussed earlier, an EMT is an Executive Management Team. This team of executives is essentially involved with the overall coordination and management of what would usually be a very highly visible and destructive disaster. An EMT would only be called together, for example, if it was necessary for the company to vacate its primary place of business and move to a disaster recovery facility. An EMT may also be brought together if the disaster posed a sticky public affairs problem, such as a hazardous chemical spill. An EMT could also be activated if a disaster were considered a threat to investors, shareholders, or customers dependent on your organization, and required a high level of public contact to assure the community that the situation was under control.

The first thing your EMT will need is a place to work. This could be a training facility, a hotel suite, or even one of the executive's homes. What is important is that the place is predefined in advance and the executives know they must report there after a disaster that renders the primary place of business unusable. Some questions to ask yourself when activating the EMT, in relation to your ability to contact them in a disaster, are as follows:

1. *Was the EMT successfully contacted?* Although this may seem academic, often in a disaster it is difficult to get in touch with key people.
2. *Do these key executives have unlisted telephone numbers, and are they documented in the plan?* Even if they do, what if telephone service is out to the area? Do they have a backup, such as a pager or a cellular phone?
3. *Did they take your notification seriously and report promptly?*

There are also subtleties involved in any type of calls to employee homes regarding disasters at the facility. For example, what if this employee was at the facility when the disaster occurred? Are the people making the calls to employee homes prepared to deal with hysterical relatives if their loved ones were at work during the disaster and this would be the first notification to them that something has happened? Therefore, check the following:

1. Was the callout procedure scripted?
2. Did individuals stick with the script?
3. Did the script work as intended or were modifications needed?

(See Figure 8.3.)

The best way to handle these questions is to provide a pre-approved checklist that not only contains names and telephone numbers but also a brief procedure to follow when contacting the employee's family. This will avoid many of the problems outlined earlier.

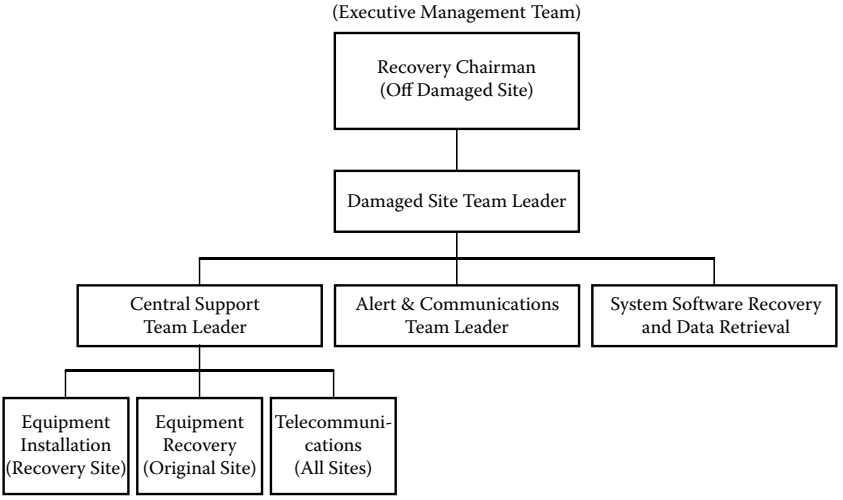


Figure 8.3 Disaster recovery organization.

Other Concerns Regarding the EMT

1. *Did the correct EMT members actually assemble at the predetermined location, or at least know where to go?*
2. *Did the EMT members require directions to the Command Center? If so, were directions to the Command Center clear and easy to follow?* This issue can be mitigated in large part by establishing the Command Center at a landmark such as a hotel or facility that is easy to find and has ready access to telephone service.
3. *Was equipment at the Command Center in time and in a usable configuration?* When the EMT arrives, a number of items must be available for use, such as telephones, fax machines, perhaps a small copier, and other things that may not be immediately apparent, such as a place to sit.
4. *Did the equipment require installation? If so, were diagrams available to technical personnel to assist in the setup of equipment?* It's not a bad idea to document the setup of the Command Center in advance, to make it a room that is not only immediately available but also conducive to a work environment for several very busy executives.
5. *Were emergency telephones easy to use?* Let's face it: one of the most ridiculous things we're faced with today is walking into an office and having to ask instructions for using the telephone. Unfortunately, this is often the case. One good way to get around this problem is to use a basic analog touch-tone telephone set. This will minimize the time spent training people on how to use the phone as well as allow them to plug in a fax, laptop, or modem, if required.
6. *Did the EMT receive critical status reports in the prescribed time frame?* Once notified of the disaster, teams will fan out citywide, or perhaps nationwide,

in implementing the company's recovery plan. These will include people dispatched to the disaster recovery center, if one is in use; another team dispatched to the affected facility to aid in restoration; and still more teams running around town to retrieve stored magnetic media, pick up and deliver equipment, and perform other functions. Most of these teams will have to deliver a report to the EMT within a designated period of time, apprising them of the damage and the progress of recovery so they can take other action as necessary. Most recovery plans will contain a statement such as the following: "The facilities restoration team will deliver a report via facsimile to the EMT within 90 minutes of arriving on site at the affected facility." Any test should include this step.

7. *Were there other areas within the organization that should have had EMT representation but did not?* Once again, the EMT should consist of a Chief Executive, a Director of Technical Services, a Building Facilities Manager, and a small administrative staff. This is a minimum. Other departments could also be involved — perhaps a representative from the real-estate department of the company, or a representative from Human Resources. Think about the makeup of the EMT and what it will take to make it more effective. Also, query executives involved in the test about other personnel they should have had there but did not.
8. *What did you learn from the exercise?* Make notes both during and after the test so that you can strengthen your recovery plan when the test is over.
9. *What will you change the next time you test?* Promptly review your recovery plan and your test procedures immediately following any test and activation. At this time, everything is fresh in your head, and your procedures can be most effectively updated.

(See Figure 8.4.)

Other Considerations

Depending on the nature of your company, it may already subscribe to a commercial recovery facility; however, not all companies do. For firms that choose not to subscribe to a commercial facility, it will be necessary to sharpen the liaison between technical services and other divisions within the company, such as real estate, which would be able to locate suitable office space quickly after a disaster.

Generally, this is not a problem, as most cities do have at least a modest surplus of office space available. It should, however, be documented in advance whenever possible. The advantage a commercial recovery center provides, naturally, is a forwarding address. This helps to form a focal point for future planning activities and makes the process much easier than just saying, "Let's assume an office suite!" The mental picture of the recovery center waiting there for the resources of the company just somehow makes the planning process easier.

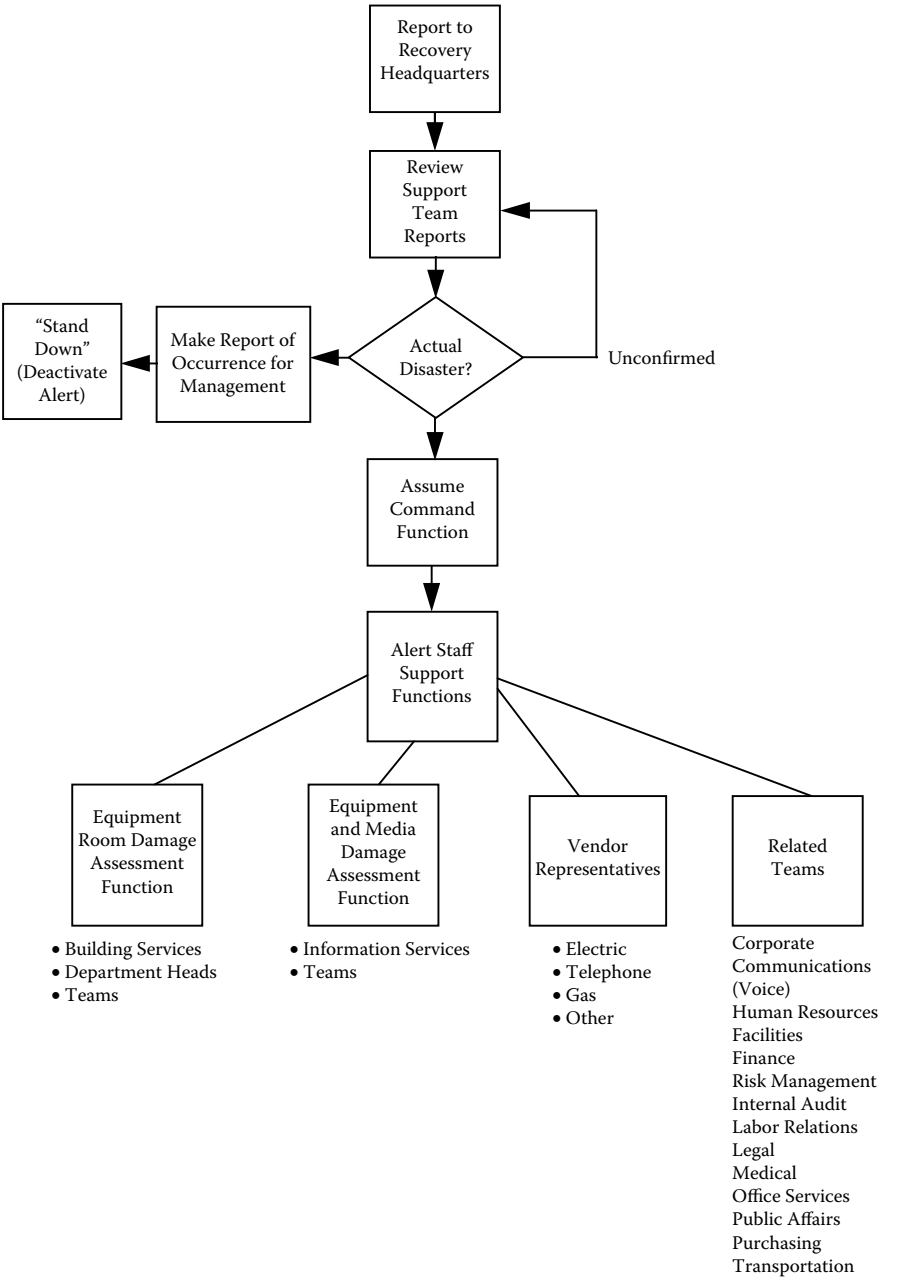
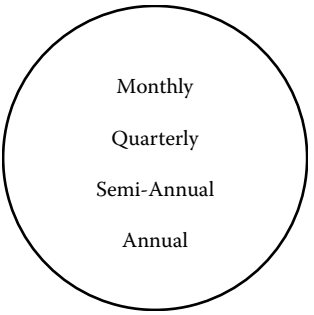


Figure 8.4 Recovery chairman's duties and responsibilities.

Many companies use off-site disaster recovery facilities from a variety of commercial sources. Although these companies are especially well adapted to this purpose, they still generally cannot single-handedly recover an organization. They will need your help. One of the questions to ask yourself when mobilizing technical service personnel involved in staffing and configuring a recovery center is, "*Were the responsible technical services teams successfully notified?*" These teams generally include the mainframe computing operation. Even though the world is full steam ahead toward distributed processing, the mainframes are still around. Because the mainframe component is generally the oldest component in the recovery plan, the entire process may, in fact, center on it. Mainframes, however, are only one component of our business, and of our recovery plan, too.

Types of Tests



Type of Test	*Example of Scope*
Monthly	Review telephone numbers and verify accuracy.
Quarterly	Internal joint test with LAN and MIS departments. (Paper only.)
Semiannual	Joint test with LAN and MIS departments. Activate backup circuits, but no live data. Use test patterns to verify continuity.
Annual	Companywide test, EMT, Facilities, Media Affairs, MIS, LAN, Telecom. If you are really BOLD, involve live data.

Other teams will also be involved, such as field services teams. These personnel, who may, for example, normally support personal computers or terminals from a maintenance standpoint, probably have the tools and training to be effectively called into service as emergency installation technicians for the new configurations. Various engineering teams, or teams of senior analysts, may also be involved to provide high-level troubleshooting and support when complex equipment configu-

rations must be built literally overnight. These are a few suggestions for technical service teams. Perhaps your recovery plan includes even more.

Assuming we're proceeding as outlined in Chapter 7, with one team dedicated to on-site restoration activities and the other team responsible for manning the recovery site, we must consider the following questions about how well these teams perform in a disaster or a test, which reveals some common errors in testing:

1. *Did the correct team members meet at the recovery center?* This can often be a problem, especially in cases of widespread disasters. Many employees will go home to ensure that their homes and families are okay before reporting to work. There, they could find injured family members, destroyed property, or a neighborhood that looks like it's prone to looting, after a widespread disaster. In cases such as these, it is not unusual at all to have less than 50 percent of your workforce show up for work.
2. *How would your recovery plan work in the absence of your key personnel?* For a very effective test, "kill" a few key personnel to simulate this happening, and see how the others compensate. The best person to nab for this would be your key technologist, or the one who immediately comes to mind as the most pivotal person in the recovery process, because of a knowledge of the environment. As this person is doing such a good job, he or she would probably enjoy an afternoon game of golf while the rest of the team tests the plan. It will also give you a good idea of how others respond without this key individual and a good indication of how well they work under stress as well. (See Figure 8.6.)
3. *Were directions to the recovery center available and easy to follow?* This is self evident, and even more important, again, in cases of widespread disaster. If the disaster is an earthquake or a flood, your employees will be delayed enough in reporting to the center without having to stop for directions. Get directions and maps from your recovery service vendor, or have these things documented in advance and put as an integral part in the recovery plan.
4. *Was the necessary equipment in a usable configuration?* Remember, the recovery center is not yours alone. Others will have been there during the time you last tested, and probably changed configurations.
5. *Were diagrams available to technical personnel to assist in the setup of equipment?* This is the context in which we've stressed in previous chapters the importance of documenting the recovery plan. Personnel who are not familiar with your day-to-day environment will want to see pictures of where the equipment goes, and exactly how to connect it. Even though your key technical people will know this, it's not guaranteed that they will be available during the disasters, or that their replacements will intuitively know this information without a detailed guide.
6. *Were recovery center personnel available and knowledgeable?* Most commercial recovery centers do an excellent job of staffing with on-site employees to show you the subtleties of complex matrix switches and other equipment that you

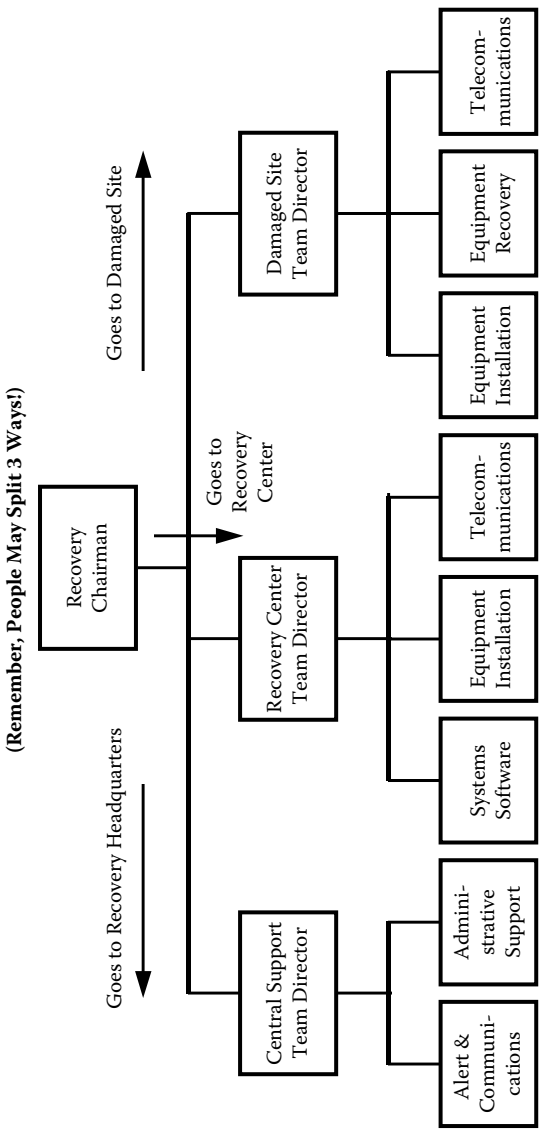


Figure 8.6 Setting up a recovery management team.

will need to use at the center. If you are using (and paying for) a recovery center, then you are evaluating this center as well as your staff in any disaster test. Commercial recovery centers are good at what they do, as a general rule, but don't come cheap. Therefore, be sure your company is getting its money's worth. Make sure that recovery center personnel are available to meet with you and serve as guides to help point out the ins and outs of operating in the center. Most of the recovery facilities, for example, make extensive use of matrix switching for telecommunications, which can be complicated to figure out without a helping hand.

7. *Was the telephone system easy to use?* Once again, the preference is for regular touch-tone, analog telephone sets. If these are not available, however, get some documentation information and train your personnel in advance to avoid unnecessary delays.
8. *Were critical status reports dispatched in the prescribed time frame to the EMT?* Always remember, the EMT must know what's going on among the teams to be in true control of the recovery process. Within 90 minutes of disaster notification, the EMT should receive a faxed, written, or verbal report from each team, both on site and at the recovery center.
9. *Were telephone help desk numbers successfully diverted?* When a large amount of technical equipment must be installed in a short timeframe, it is very helpful to keep the same help desk or network control number. This way, vendors supporting your recovery process can contact you easily and not have to learn new numbers. This avoids other unnecessary delays.
10. *Was dial-in data service successfully established?* Many companies use some type of dial-in data communication service. Modems should not be a concern, as these are fairly standardized and readily available from a variety of sources. Therefore, concentrate on the telephone numbers; just as with voice telephone numbers, modem numbers should not change. These numbers can be diverted either by the local telephone operating company or long-distance carrier to any ten-digit working number in North America. As commercial recovery companies have hundreds, or perhaps thousands, of such numbers, there is not really an excuse for not restoring this circuit promptly, provided you learn the numbers in advance and preplan.
11. *Were T1, T3, and SONET loops intact, and were these properly optioned?* Check the complement of telecommunications services you have in support of data transmission for your users, and be sure to plan in advance. One common problem with T1s, for example, centers around the fact that most T1 local loops to recovery centers are, once again, shared among a broad user community. As each customer using these link tests may be using a different line code for the T1, the links may have been re-optioned since you last tested and will not work without modification. Procedures for re-optioning CSUs, and other components that may have changed should be detailed in the plan. The best test in all of these cases is a live test. Even if live production data is

not transmitted, it is a good idea to run a test pattern across these facilities to assure that the telecommunications facilities are intact, work properly, and would support your data if it ever became necessary.

12. *Was data stored off-site successfully delivered to the recovery center for the following items?* Most companies have procedures for the off-site storage of mainframe data and have regular pick-up schedules for the tapes. Data residing on "open systems" can be somewhat "iffier," however. Sometimes, a LAN Administrator will make a backup and simply take the tape home, rather than include it in a formal pickup schedule. This is fine insofar as it does get the tape off site; however, what happens if the LAN Administrator goes with the building in a disaster? Would you or one of your people like to be the one to go to that LAN Administrator's house, knock on the door, and tell a tearful wife, "I'm sure sorry that your husband passed away today, but we need to shake your house down for that tape." Once again, I realize this sounds a little tongue-in-cheek, but it does underscore the point. Secondly, with any type of off-site storage facility, mobility could be a problem. If you happen to be on the West Coast, it will be difficult to get anywhere after an earthquake if bridges are down, traffic lights don't work, and there's eight feet of glass in the street! Don't be afraid to introduce these types of complications into your testing procedure. For example, as part of the script for the test, instruct employees to retrieve off-site storage data as usual, "but don't use Main Street," for example.
13. *Was data stored off-site for telecommunications switches, PBXs, multiplexers, etc.*? As stated elsewhere in the book, it's a tough enough job to recover a 1000-line telephone switch quickly in the event of a disaster. Even worse is figuring out who had what telephone number because this information was not stored off site. Similar problems exist for sophisticated multiplexer equipment, which is also largely software-defined these days.
14. *Does your voice mail system reside on site?* Voice mail can be indispensable for command and control in a disaster. However, if your voice mail system resides on site, chances are it could be affected in a buildingwide disaster. Perhaps fallback procedures could be put in place to use a commercial voice mail vendor and your normal telephone numbers call-forwarded to allow transparent use. Remember, give yourself every advantage for command and control.
15. *Automated call distribution (ACD) units?* These are highly customized and heavily software-driven pieces of equipment. Therefore, their restoration in a disaster could be slow. Take an especially hard look at these, both before and during a test, because they are complicated, and generally support your core business, such as incoming sales groups.
16. *Expect problems with the installation or restoration of software.* Anyone who's been involved in any type of a recovery center test knows that this is a very common problem. Small subtleties and operating systems, or even minute

differences in components such as tape drives, can create lasting and severe headaches for people attempting to deinstall software from one system and reinstall it on another. You will undoubtedly learn many shortcuts in this process that work toward a more graceful reload on the new systems.

17. *Was test equipment available?* If not, what will you need next time? We have all had the experience of being in our garage working on some project and suddenly not having the proper tool to finish the job. The same holds true with the recovery process. Be sure your people have the proper tools to do what they are there to do.
18. *Did test equipment on hand at the recovery center function properly?* The recovery service vendor probably has test equipment installed at the center for general use. If so, go out and presurvey this equipment in advance, and be sure it's suitable or adaptable to the processes you intend.
19. *Were proper small items, such as hand tools, available and adequate?* What would your recovery process be like, for example, if the personnel at the recovery center could not find a pair of pliers, note pad, or other seemingly insignificant items? Make a note of these if they are not available during the test, so that they will be the next time.
20. *Was response by equipment vendors prompt and adequate?* It is highly recommended that your company contact its principal equipment vendors and ask for an on-site representative at the recovery center. When this is done, rate the vendors on how supportive they were in their response. If your company has vendor-sponsored disaster recovery programs, or roll-in replacement guarantees, now is the time to implement them. Pay careful attention to the performance of your vendors, and be sure that they deliver everything that they say they can.
21. *Were any equipment service or installation manuals required?* Remember that your people will be out at the recovery center installing a system, probably overnight, that originally took years to create. Give them every advantage.
22. *Was the overall environment at the recovery center reasonably conducive to our company's work environment?* In other words, could you get your job done there? Could you get your job done there over time?
23. *Were there other areas of the organization that should have been represented at the center but were not?* Or, stated another way, was anyone represented at the center who was not really required to be there? These two items speak to the issue of effectively utilizing your personnel. Someone who may be a fifth wheel at the recovery center could possibly be more effectively utilized at the damaged facility as part of the restoration effort. Personnel will be at a premium in any recovery center test or activation, so be sure to use them properly and most efficiently.
24. *What did you learn?* Even the most advanced organizations learn something every time they test the recovery plan. In fact, if your organization consistently produces flawless results on its recovery tests, this probably indicates that it's time to tighten the standards. Be sure that your management understands that

you are going to test your plan until you fail to make it a true test. After each test, document what you learned from the activation and the items you would change for the next test, so as to allow that one to go even more gracefully. We again stress the importance of opening a critical events log (a $0.29 school-type paper notebook to log command decisions) as soon as you are notified of a disaster. This makes for a convenient review, after a disaster or test, to tighten up on procedures that could have gone better or to codify issues that came to mind during the process, which would make a good part of the plan. The Critical Events Log, if a notebook is used, can be easily tucked into the jacket of a written disaster recovery plan, where it will hopefully find immediate use when the plan is activated.

Hopefully, these suggestions may prove to be helpful when your company first activates its recovery plan. Don't expect everything to go perfectly; in fact, you may want to alert management to expect perhaps a not-so-perfect test. It will be rough the first couple of times out. Afterward, however, employees will learn by doing, and the plan will run smoother. When the activations start to run consistently smoother, it's time to tighten the criteria.

As stated earlier, imagine the disaster has reduced staff by an employee or two, and see how things operate then, or forbid employees to use certain disaster-impacted streets, for example, when implementing the plan. Introducing complications such as these will stress the plan, with the idea being the "the company tests until it fails." Once a plan component does fail, procedures can be strengthened to keep the same thing from happening the next time. By producing failures during the testing procedures, the company can be more secure in the knowledge that the plan will work when it's really needed, under actual disaster conditions.

TRAINING CONSIDERATIONS

1. Do you make BCP training mandatory? Is it mandatory? Do you train:
   a. Team members?
   b. Carriers?
   c. Vendors?
   d. Executive management team?
   e. New hires?
2. How do you train them?
   a. Newsletter/memo
   b. On-site classes
   c. Off-site seminars
   d. Videotapes

SPECIAL SECTION — LEGAL IMPLICATIONS OF NOT ADEQUATELY PLANNING

Chapter 9

Legal and Regulatory Requirements Regarding Disaster Recovery Planning

Eddie M. Pope

Contents

Introduction 272
How to Use This Chapter 273
Companies That Are Required to Have Disaster Recovery Plans 273
Companies That Are Required to Have Some Elements of a Disaster Recovery Plan 282
Preparedness Planning Is Encouraged by Law 293
Preparedness Planning for the Legal Department 306
Appendix A: Best Practices 311
Appendix B: IRS Rev. Procedure 98-25 312
Appendix C: Financial Institution Rules from GLB 323
Appendix D: Checklist for Pandemic Planning 326

Introduction

First, let me introduce myself. My name is Ed Pope. I am trained as a lawyer and have over 25 years' experience practicing law in several settings: as a government lawyer, in-house counsel, and big law firm attorney. I've now come to believe that disaster recovery planning is more important than practicing law. Katrina and Rita convinced me that we can no longer rely upon the government in the immediate aftermath of a disaster. In the first week or two after a disaster, it will be up to individuals and businesses to do what is necessary to save lives and restore property. As you will see in this chapter, some companies — banks and other financial institutions, stockbrokers, electric and telephone companies — are required to have plans to do just that. I believe that *every* company that is large enough to have fire drills or keep an inventory should have a disaster recovery plan.

I think it's important to tell you that belief right up front, as it is my experience that people tend to "find" the law as they think it ought to be, rather than as it truly *is.* In researching this chapter, for example, I found several sites that said that defense contractors needed to have a disaster recovery plan. Makes sense — makes a *lot* of sense, in fact — but I couldn't find a law, rule, or regulation that actually *said* that. Until someone actually shows me such a rule or regulation, I'm going to assume that it is the disaster recovery communities' equivalent of an urban myth — a story that is passed along from planner to planner without anyone ever tracking back to see if it's true. For every statute or rule in this chapter, I've actually tracked it back to the original source. I've given you the "citation" to the statute or regulation — sort of its address for lawyers — so that if you find a statute or regulation that looks like it might apply to your business, you can take it to your lawyer and get his or her opinion as to whether it *really* applies. In most instances, I've given you the *exact* language of the regulation. As far as I know, this is the first time all of those regulations have been pulled together in one place.

It is important for me to say at this point in the chapter that I am *not* providing legal advice. No book can provide such advice because it is necessary to apply the law to the facts to know exactly how (or whether) the law governs your situation. Sometimes the law can appear to say something, even very clearly, but an experienced lawyer will know of some other exception or case that says a statute does not really "mean" what it appears to say. This book is also limited; I'm only looking at federal laws and federal regulations. There may be state laws that require planning that I have not captured in this chapter. Furthermore, as soon as this book goes to print, it is dated. New laws and new regulations are being adopted every day, and there is no way any book can keep up with all of the changes.

Finally, even though I've tried to track down every law I can that might relate to disaster recovery planning, there are a myriad of terms in the law and the industry that might apply, and I may have missed one. For example, this book discusses "disaster recovery planning," which is also known as "business resumption planning," "business resiliency planning," "crisis management," "continuity

of operations planning," "emergency response planning," "contingency planning," "business risk analysis," etc. If a law or a regulation includes a term that I didn't know about, it isn't in this chapter, but it still might apply to your business. If you do know of a law or regulation that I've missed, please let me know at empope@tellawcomlabs.com. I'll send you a gift and include a credit in the next editions of this book.

How to Use This Chapter

I've divided the rest of this chapter into five parts. I expect that very few people will read all five parts. If your company is one of the ones that is required to have a full disaster recovery plan by federal law or regulation, I have included it in Section 3 of this chapter. If your company is required to have *some* elements of a plan — for example, an emergency response to a hazardous spill — I've included it in Section 4. Section 5 talks about laws and regulations that *recommend* disaster recovery planning. Finally, Section 6 is aimed at those companies that have in-house legal departments. If you have lawyers that work for your company, please let them read that chapter.

You will want to look at the parts that apply to your type of company. If you do not see your type of company listed in Sections 3 or 4, I suggest that you read Section 5. Even if you do see your company listed in Section 4, I recommend that you at least look at discussion of NFPA 1600 in Section 5. It is my belief that the standards contained in NFPA 1600 will ultimately be incorporated into regulations for companies that do business with the federal government or that are regulated in one way or other by federal law. Following NFPA 1600 is also a prudent business practice.

If you are reading this chapter, you are now responsible for your company. Whether or not your business will survive a disaster is in *your* hands. You are responsible for the safety of your employees or coworkers. You are responsible for the survival of critical business records. How fast your business will "bounce back" if a disaster strikes is up to you. If you don't believe that you have the authorization to implement a business resumption plan, then hand this book to someone who can get that authorization. It is up to *you* to take action now!

Companies That Are Required to Have Disaster Recovery Plans

The following types of companies are required to have disaster recovery plans by virtue of federal law or regulation. This is only a summary of the requirements. Where such materials are available on the Web, I have included links to additional resources.

Banks, Credit Unions, and Other Financial Institutions

The Federal Financial Institutions Examination Council (the Council) was established on March 10, 1979, pursuant to title X of the Financial Institutions Regulatory and Interest Rate Control Act of 1978 (FIRA), Public Law 95-630. In 1989, title XI of the Financial Institutions Reform, Recovery, and Enforcement Act of 1989 (FIRREA) established the Council.

The Council is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), 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) and to make recommendations to promote uniformity in the supervision of financial institutions. In other words, every bank, savings and loan, credit union, and other financial institution is governed by the principles adopted by the Council.

In March of 2003, the Council released its *Business Continuity Planning Handbook* designed to provide guidance and examination procedures for examiners in evaluating financial institution and service-provider risk-management processes. The entire *Business Continuity Planning Handbook* published by the Council can be found at http://www.occ.treas.gov/efiles/disk2/handbooks/bcp/bus_continuity_plan.pdf. Although it is characterized as a guide for examiners evaluating financial institutions, it is actually written as a guide for the Board and management of such institutions. The following discussion is just a summary of the *Handbook*; interested readers should review the entire document for details and checklists associated with the creation of a compliant business continuity plan.

The Introduction to the *Handbook* explains the importance of what it calls business continuity planning:

> Business continuity planning is the process whereby financial institutions ensure the maintenance or recovery of operations, including services to customers, when confronted with adverse events such as natural disasters, technological failures, human error, or terrorism. The objectives of a business continuity plan (BCP) are to minimize financial loss to the institution; continue to serve customers and financial market participants; and mitigate the negative effects disruptions can have on an institution's strategic plans, reputation, operations, liquidity, credit quality, market position, and ability to remain in compliance with applicable laws and regulations. Changing business processes (internally to the institution and externally among interdependent financial services companies) and new threat scenarios require financial institutions to maintain updated and viable BCPs.

Responsibilities of the Board and Senior Management

The *Handbook* makes it clear that the responsibility for business continuity planning starts at the Board level and carries through to senior management. The *Handbook* summarizes the responsibilities as follows:

- Allocating sufficient resources and knowledgeable personnel to develop the BCP
- Setting policy by determining how the institution will manage and control identified risks
- Reviewing BCP test results
- Approving the BCP on an annual basis
- Ensuring the BCP is kept up to date, and employees are trained and aware of their role in its implementation

The BCP Planning Process

The *Handbook* sets the following goals for the planning process:

- Business continuity planning is about maintaining, resuming, and recovering the business, not just the recovery of the technology.
- The planning process should be conducted on an enterprisewide basis.
- A thorough business impact analysis and risk assessment are the foundation of an effective BCP.
- The effectiveness of a BCP can only be validated through testing or practical application.
- The BCP and test results should be subjected to an independent audit and reviewed by the board of directors.
- A BCP should be periodically updated to reflect and respond to changes in the financial institution or its service providers.

The Business Impact Analysis

As noted in the preceding text, the first step of a viable BCP is a Business Impact Analysis (BIA). The amount of time and effort necessary to conduct such a BIA will vary from institution to institution. The key action items associated with the BIA are

- Identification of the potential impact of uncontrolled, nonspecific events on the institution's business processes and its customers
- Consideration of all departments and business functions, not just data processing
- Estimation of maximum allowable downtime and acceptable levels of data, operations, and financial losses

In creating a BIA, Departments should consider the following questions:

- What specialized equipment is required, and how is it used?
- How would the department function if mainframe, network, or Internet access were not available?
- What single points of failure exist, and how significant are those risks?
- What are the critical outsourced relationships and dependencies?
- What is the minimum number of staff and space that would be required at a recovery site?
- What special forms or supplies would be needed at a recovery site?
- What communication devices would be needed at a recovery site?
- What critical operational or security controls require implementation prior to recovery?
- Is there any potential impact from common recovery sites serving multiple lines of business or departments?
- Have employees received cross training, and has the department defined backup functions/roles employees should perform if key personnel are not available?
- Are emotional support and family care needs adequately considered?

The Risk Assessment

The second step in implementing a BCP plan that would comply with the *Handbook* is a Risk Assessment. The action items for the Risk Assessment are

- A prioritizing of potential business disruptions based upon severity and likelihood of occurrence
- A gap analysis comparing the institution's existing BCP, if any, to what is necessary to achieve recovery time and point objectives
- An analysis of threats based upon the impact on the institution, its customers, and the financial markets — not just the nature of the threat

The *Handbook* explains

> Threat scenarios need to consider the impact of a disruption and probability of the threat occurring. Threats range from those with a high probability of occurrence and low impact to the institution (e.g., brief power interruptions), to those with a low probability of occurrence and high impact on the institution (e.g., hurricane, terrorism). High probability threats are often supported by very specific BCPs. However, the most difficult threats to address are those that have a high impact on the institution but a low probability of occurrence.

Development of the Business Continuity Plan

Once the organization has done a BIA and a risk assessment, it is ready to craft a BCP. The objective of the plan is to maintain, resume, and recover critical business functions. The Action Summary specifies that the BCP is to be

- Written and disseminated so that various groups of personnel can implement it in a timely manner
- Specific regarding what conditions should prompt implementation of the plan
- Specific regarding what immediate steps should be taken during a disruption
- Flexible to respond to unanticipated threat scenarios and changing internal conditions
- Focused on how to get the business up and running in the event that a specific facility or function is disrupted, rather than on the precise nature of the disruption
- Effective in minimizing service disruptions and financial loss

Other Policies, Standards, and Processes

The *Handbook* makes clear that the institution's BCP does not stand alone. It should be integrated into other institutional planning and procedures. The *Handbook* points out that the financial institution should make sure that the BCP is compliant with the system development life cycles; change control policies; data synchronization procedures; employee training and communication plans; insurance policies; government, media, and community relations policies; and security. It is sufficient to the purposes of this chapter to point out that the institution's BCP is expected to integrate these areas. An institution that is required to follow the *Handbook* should examine it for the details of such integration.

Risk Monitoring

The final step in BCP planning is Risk Monitoring. In other words, the BCP is not intended to simply sit on a shelf. Risk monitoring involves the following actions that insure that the plan is viable:

- Testing the BCP at least annually
- Subjecting the BCP to independent audit and review
- Updating the BCP based upon changes to personnel and the internal and external environments

The *Handbook* provides several pages of explanation as to the overall testing strategy, the testing scope and objectives, the test plan review, the validation of

assumptions, the accuracy of information, and completeness of procedures. It specifies the types of testing methods that should be considered, including an orientation/walk-through, a "table-top" mini-drill, functional testing, and a full-scale test. It also gives guidelines on conducting the test and reporting and analyzing the test results.

The *Handbook* emphasizes that a BCP is a "living" document. It should be updated at least annually, with the review including the senior management and the Board of Directors. Updates should reflect changes to the institution's business, structure, systems, software, hardware, personnel, or facilities. Furthermore, it should be reviewed by outside auditors or experts in such plans to make sure that the Board's objectives are being met. The outside expert should be allowed to directly observe the testing of the BCP.

Stock Brokers, Dealers, and Similar Firms

The National Association of Securities Dealers (NASD) has adopted rules that require all of its members to have BCPs. The NASD oversees the activities of more than 5,100 brokerage firms, approximately 130,800 branch offices, and more than 658,770 registered securities representatives. As of June 14, 2004, the rules apply to all NASD member firms. (It is important to note that the rules apply to every company that deals in securities, such as brokers, dealers, and their representatives; it does not apply to the listed companies themselves.) The requirements are specified in Rule 3510 and 3520.

Rule 3510 has the following provisions:

3510 — Business Continuity Plans

(a) Each member must create and maintain a written BCP identifying procedures relating to an emergency or significant business disruption. Such procedures must be reasonably designed to enable the member to meet its existing obligations to customers. In addition, such procedures must address the member's existing relationships with other broker-dealers and counter-parties. The BCP must be made available promptly upon request to NASD staff.

(b) Each member must update its plan in the event of any material change to the member's operations, structure, business, or location. Each member must also conduct an annual review of its business continuity plan to determine whether any modifications are necessary in light of changes to the member's operations, structure, business, or location.

(c) The elements that comprise a BCP are flexible and may be tailored to the size and needs of a member. Each plan, however, must, at a minimum, address
   (1) Data backup and recovery (hard copy and electronic).
   (2) All mission-critical systems.
   (3) Financial and operational assessments.

(4) Alternate communications between customers and the member.
(5) Alternate communications between the member and its employees.
(6) Alternate physical location of employees.
(7) Critical business constituent, bank, and counter-party impact.
(8) Regulatory reporting.
(9) Communications with regulators.
(10) How the member will assure customers' prompt access to their funds and securities in the event the member determines that it is unable to continue its business.

Each member must address the just-listed categories to the extent applicable and necessary. If any of the just-listed categories is not applicable, the member's BCP need not address the category. The member's BCP, however, must document the rationale for not including such category in its plan. If a member relies on another entity for any one of the just-listed categories or any mission- critical system, the member's BCP must address this relationship.

(d) Members must designate a member of senior management to approve the plan, and he or she shall be responsible for conducting the required annual review. This member of senior management must also be a registered principal.
(e) Each member must disclose to its customers how its BCP addresses the possibility of a future significant business disruption and how the member plans to respond to events of varying scope. At a minimum, such disclosure must be made in writing to customers at account opening, posted on the member's Internet Web site (if the member maintains a Web site), and mailed to customers upon request.
(f) For purposes of this rule, the following terms shall have the meanings specified:
(1) *Mission-critical system* means any system that is necessary, depending on the nature of a member's business, to ensure prompt and accurate processing of securities transactions, including, but not limited to, order taking, order entry, execution, comparison, allocation, clearance and settlement of securities transactions, maintenance of customer accounts, access to customer accounts, and delivery of funds and securities.
(2) *Financial and operational assessment* means a set of written procedures that allow a member to identify changes in its operational, financial, and credit risk exposures.

Rule 3520 requires the maintenance of the following emergency contact information:

3520 — Emergency Contact Information

(a) Each member shall report to NASD, via such electronic or other means as NASD may require, prescribed emergency contact information for the

member. The emergency contact information for the member includes designation of two emergency contact persons. Each emergency contact person shall be a member of senior management and a registered principal of the member.

(b) Each member must promptly update its emergency contact information, via such electronic or other means as NASD may require, in the event of any material change. Each member must review and, if necessary, update its emergency contact information, including designation of two emergency contact persons, within 17 business days after the end of each calendar quarter to ensure the information's accuracy. The member's Executive Representative, or his or her designee, which designation must be in writing, must conduct such review and any update. Furthermore, members must have adequate controls and procedures to ensure that only the Executive Representative, or his or her written designee, may perform the review and update.

Additional resources for NASD firms preparing a business continuity plan can be found at http://www.nasd.com/web/idcplg?IdcService=SS_GET_PAGE&nodeId=649. That page includes:

- BCP FAQs
- NASD Small Firm Business Continuity Plan Template
- An example of BCP Disclosure Statement for introducing firms with a clearing firm arrangement
- BCP Repository Service
- BCP Case Study (PDF 81 KB), an exercise to help frame your BCP planning

Member firms may want to explore the BCP Repository Service. As explained by the NASD,

> Recognizing that not all firms have a secure, off-site facility to store and update their BCP, NASD has arranged for EVault, a leading provider of network backup and recovery software and services, to provide this voluntary electronic repository service specifically designed for NASD firms.

The BCP Repository Service, powered by EVault and offered in association with NASD, provides

Highly secure, off-site storage for BCPs
The ability to upload and modify documents from anywhere with an Internet connection
Document collaboration across authorized users
Highly secure, over-the-wire encryption of all uploaded and downloaded documents

Firms will also have the option of allowing NASD staff to access critical business continuity materials in times of business disruption. Firms electing this option will have two folders in their vault — one for NASD access and one that is private and only accessible by the firm. EVault will offer this service to firms for a fee of $144 per year ($12 per month) for 200MB of available electronic storage space, with a one-time setup fee of $25.

Electric Utilities

The reliability function relating to the electric utility grid is undergoing a change. Prior to 2005, the Federal Energy Regulatory Commission (FERC) could only coordinate volunteer efforts between utilities for reliability. That changed with the adoption of Title XII of the Energy Policy Act of 2005 (16 U.S.C. 824o). That law now authorizes the FERC to create an Electric Reliability Organization (ERO). The ERO will have the ability to adopt and enforce reliability standards for "all users, owners, and operators of the bulk power system" in the United States.

As this chapter is being written, the FERC is in the process of finalizing the rules for the creation of the ERO. Once the ERO is created, it will begin the process of establishing reliability standards. It is very safe to assume that the ERO will adopt standards for service restoration and the appropriate utility response to disasters. Every electric utility already has such plans on a voluntary basis, and utilities have traditionally worked together across service-area boundaries to assist fellow utilities in times of need.

Telecommunications Utilities

Telecommunications utilities are governed at the federal level by the Federal Communications Commission (FCC). The FCC, in turn, has created the Network Reliability and Interoperability Council (NRIC). The role of the NRIC is to develop recommendations for the FCC and the telecommunications industry to "insure optimal reliability, security, interoperability and interconnectivity of, and accessibility to, public communications networks and the internet." The NRIC's members are senior representatives of providers and users of telecommunications services and products, including telecommunications carriers; the satellite, cable television, wireless and computer industries; trade associations; labor and consumer representatives; manufacturers; research organizations; and government-related organizations.

The NRIC has adopted a list of 803 "best practices." A full list of the best practices can be found at http://www.bell-labs.com/cgi-user/krauscher/bestp.pl?howDisp=&allrecords=allrecords.

The NRIC makes it abundantly clear that its best practices are not mandatory. The opening screen for the list of best practices contains this notice:

> Implementation of NRIC Best Practices is voluntary. The implementation decision is left with the responsible organization and is to be made by individuals with sufficient competence to understand them. Mandated implementation of these Best Practices is not consistent with their intent.

Even though this warning appears to make the best practices voluntary, I believe the telecommunications industry as a whole has a good history of having disaster recovery plans. Therefore, I have included the list of "best practices" primarily related to disaster recovery and emergency planning for the industry as "Appendix A" to this chapter.

Companies That Are Required to Have Some Elements of a Disaster Recovery Plan

Whereas highly regulated entities such as banks, credit unions, stock brokers, and utilities have rules or industry standards that require a "full" disaster recovery plan, there are numerous industries that are required to have some elements of such a plan. For the most part, these requirements relate to the ability to maintain data in a secure manner and retrieve it quickly after a disaster has occurred.

Providers of Health Services — HIPAA

HIPAA stands for the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, which amended the Internal Revenue Service Code of 1986. A good explanation of how HIPAA came about can be found at http://www.healthdatamanagement.com/HDMSearchResultsDetails.cfm?articleId=8126. Also known as the Kennedy–Kassenbaum Act, it includes a section, Title II, entitled Administrative Simplification, requiring

> Improved efficiency in healthcare delivery by standardizing electronic data interchange, and protection of confidentiality and security of health data through setting and enforcing standards.

The legislation called upon the Department of Health and Human Services (HHS) to publish new rules that will ensure security standards protecting the confidentiality and integrity of "individually identifiable health information," past, present, or future.

The final Security Rule was published by HHS on February 20, 2003, and provides for a uniform level of protection of all health information that is housed or transmitted electronically and that pertains to an individual. The Security Rule requires covered entities to ensure the confidentiality, integrity, and availability of all electronic protected health information (ePHI) the covered entity creates, receives, maintains, or transmits. It also requires entities to protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI, protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required by the Privacy Rule, and ensure compliance by their workforce. Required safeguards include application of appropriate policies and procedures, safeguarding physical access to ePHI, and ensuring that technical security measures are in place to protect networks, computers, and other electronic devices.

Some parties were opposed to the adoption of mandated contingency plans. In response, the HHS reasoned:

> A contingency plan is the only way to protect the availability, integrity, and security of data during unexpected negative events. Data are often most exposed in these events, since the usual security measures may be disabled, ignored, or not observed.
>
> Each entity needs to determine its own risk in the event of an emergency that would result in a loss of operations. A contingency plan may involve highly complex processes in one processing site, or simple manual processes in another. The contents of any given contingency plan will depend upon the nature and configuration of the entity devising it.

The HIPAA security rule applies to virtually every provider of health services, including health plans, health care clearinghouses, and health care providers who transmit health information. Some parts of the security plan also apply to entities that deal with the patient's health information, such as pharmacies. My former law firm, for example, would obtain health information about individuals in the course of preparing for litigation. It was required to satisfy some of the HIPAA security requirements.

The portion of the regulations that deal with contingency planning and disaster recovery planning is 45 CFR 164.308(a)(7). Those standards provide for implementation specifics that are either "required" or "addressable." My non-expert interpretation of those terms is that a covered entity must be able to demonstrate compliance with a "required" standard, but may be able to show that an "addressable" standard does not apply to its particular situation. The rules provide

(7)(i) Standard: Contingency plan. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

(ii) Implementation specifications:

(A) Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

(B) Disaster recovery plan (Required). Establish (and implement as needed) procedures to restore any loss of data.

(C) Emergency mode operation plan (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

(D) Testing and revision procedures (Addressable). Implement procedures for periodic testing and revision of contingency plans.

(E) Applications and data criticality analysis (Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components.

Entities that are subject to the HIPAA security standards should note that they only apply to electronic protected health information. That is why I have placed them in the "some" planning is required. The standards do not technically apply to other business records of the health care provider. It seems logical to me that if an institution is going to go through the process of preparing a contingency plan, it should go beyond the bare bones of HIPAA and cover *all* critical operations of the entity in question.

Entities that are governed by HIPAA should also be aware that the portion of the rules quoted in the preceding text is only a small portion of the security regulations, which are only a small part of all the HIPAA regulations.

Employers with More than Ten Employees — OSHA

The U.S. Department of Labor has adopted numerous rules and regulations in regard to workplace safety as part of the Occupational Safety and Health Act. That Act (29 USC 654) requires that

(a) Each employer —

(1) shall furnish to each of his employees employment and a place of employment which are free from recognized hazards that are causing or are likely to cause death or serious physical harm to his employees;

(2) shall comply with occupational safety and health standards promulgated under this Act.

(b) Each employee shall comply with occupational safety and health standards and all rules, regulations, and orders issued pursuant to this Act.

The specific rule requiring emergency planning can be found at 29 CFR 1910.38. The OSHA Web site (www.osha.gov) displays the rule in this manner:
1910.38(a)
Application. An employer must have an emergency action plan whenever an OSHA standard in this part requires one. The requirements in this section apply to each such emergency action plan.
1910.38(b)
Written and oral emergency action plans. An emergency action plan must be in writing, kept in the workplace, and available to employees for review. However, an employer with 10 or fewer employees may communicate the plan orally to employees.
1910.38(c)
Minimum elements of an emergency action plan. An emergency action plan must include at a minimum:
1910.38(c)(1): Procedures for reporting a fire or other emergency
1910.38(c)(2): Procedures for emergency evacuation, including type of evacuation and exit route assignments
1910.38(c)(3): Procedures to be followed by employees who remain to operate critical plant operations before they evacuate
1910.38(c)(4): Procedures to account for all employees after evacuation
1910.38(c)(5): Procedures to be followed by employees performing rescue or medical duties
1910.38(c)(6): The name or job title of every employee who may be contacted by employees who need more information about the plan or an explanation of their duties under the plan
1910.38(d)
Employee alarm system. An employer must have and maintain an employee alarm system. The employee alarm system must use a distinctive signal for each purpose and comply with the requirements in § 1910.165.
1910.38(e)
Training. An employer must designate and train employees to assist in a safe and orderly evacuation of other employees.
1910.38(f)
Review of emergency action plan. An employer must review the emergency action plan with each employee covered by the plan:
1910.38(f)(1): When the plan is developed or the employee is assigned initially to a job
1910.38(f)(2): When the employee's responsibilities under the plan change
1910.38(f)(3): When the plan is changed

In addition to the formal rules that all employers are required to follow, the rules also contain an appendix containing a "nonmandatory guideline" to assist employers

in complying with the formal rules. The guideline can be found at http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=STANDARDS&p_id=10114. The guideline provides more information about what is expected to be covered with an emergency plan. "The emergency action plan should address emergencies that the employer may reasonably expect in the workplace. Examples are: fire; toxic chemical releases; hurricanes; tornadoes; blizzards; floods; and others." The guideline recommends in an emergency plan detail which employees are to stay behind in order to care for "essential plant operations." The guidelines also define *essential plant operations*:

> Essential plant operations may include the monitoring of plant power supplies, water supplies, and other essential services which cannot be shut down for every emergency alarm. Essential plant operations may also include chemical or manufacturing processes which must be shut down in stages or steps where certain employees must be present to assure that safe shut down procedures are completed.

The guideline suggests the use of floor maps that show emergency evacuation routes and the designation of certain employees for rescue and medical first-aid duties. It recognizes that there are different levels of evacuation necessary for different levels of emergency. It encourages the determination of refuge or safe areas, which may be outside the plant. The guidelines also provide helpful advice regarding "emergency action plan training," "fire prevention housekeeping," and maintenance of equipment under the fire prevention plan."

OSHA has many other regulations that impact upon emergency response planning and employee protection. One OSHA site lists these rules as pertaining to emergency response:

Some OSHA Requirements

The following is a list of some of the OSHA requirements pertaining to emergency response. These references refer to appropriate sections of the Occupational Safety and Health Standards (*Title 29, Code of Federal Regulations, Part 1910*, which are the OSHA General Industry Standards).

Subpart E — Means of Egress
1910.37 Means of egress
1910.38 Employee emergency plans and fire prevention plans
Appendix to Subpart E — Means of egress
Subpart H — Hazardous Materials
1910.119 Process safety management of highly hazardous chemicals
1910.120 Hazardous waste operations and emergency response

Subpart I — Personal Protective Equipment
1910.132 General requirements — personnel protection
1910.133 Eye and face protection
1910.134 Respiratory protection
1910.135 Occupational head protection
1910.136 Occupational foot protection
1910.138 Hand protection
Subpart J — General Environmental Controls
1910.146 Permit-required confined spaces
1910.147 Control of hazardous energy sources
Subpart K — Medical and First Aid
1910.151 Medical services and first aid
Subpart L — Fire Protection
1910.155–156 Fire protection and fire brigades
1910.157–163 Fire suppression equipment
1910.164 Fire detection systems
1910.165 Employee alarm systems
Appendix A–E of Subpart L
Subpart R — Special Industries, Electrical Power
Generation, Transmission, and Distribution
Subpart Z — Toxic and Hazardous Substances
1910.1030 Bloodborne pathogens
1910.1200 Hazard communication

The OSHA Web site has numerous materials that are designed to help businesses comply with the various rules and regulations. One helpful site is http://www.osha.gov/SLTC/smallbusiness/sec10.pdf.

Foreign Corrupt Practices Act

The Foreign Corrupt Practices Act of 1977 (FCPA), 15 U.S.C. §§ 78dd-1, *et. seq* prohibits corrupt payments to foreign officials for the purpose of obtaining or keeping business. As a result of SEC investigations in the mid-1970s, over 400 U.S. companies admitted making questionable or illegal payments in excess of $300 million to foreign government officials, politicians, and political parties. The abuses ran the gamut from bribery of high foreign officials to secure some type of favorable action by a foreign government to so-called facilitating payments that allegedly were made to ensure that government functionaries discharged certain ministerial or clerical duties. Congress enacted the FCPA to bring a halt to the bribery of foreign officials and to restore public confidence in the integrity of the American business system. The Department of Justice is the chief enforcement agency, with a coordinate role played by the Securities and Exchange Commission (SEC). The Office of General

Counsel of the Department of Commerce also answers general questions from U.S. exporters concerning the FCPA's basic requirements and constraints.

The FCPA was intended to have, and has had, an enormous impact on the way American firms do business. Several firms that paid bribes to foreign officials have been the subject of criminal and civil enforcement actions, resulting in large fines and suspension and debarment from federal procurement contracting, and their employees and officers have gone to jail.

The provision of the FCPA that has been cited as requiring disaster recovery planning is 15 USC 78m (b)(2), which provides:

(2) Every issuer which has a class of securities registered pursuant to section 78l of this title and every issuer which is required to file reports pursuant to section 78o(d) of this title shall —
  (A) Make and keep books, records, and accounts, which, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the issuer.
  (B) Devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that —
    (i) Transactions are executed in accordance with management's general or specific authorization.
    (ii) Transactions are recorded as necessary (I) to permit preparation of financial statements in conformity with generally accepted accounting principles or any other criteria applicable to such statements, and (II) to maintain accountability for assets.
    (iii) Access to assets is permitted only in accordance with management's general or specific authorization.
    (iv) The recorded accountability for assets is compared with the existing assets at reasonable intervals and appropriate action is taken with respect to any differences.

As used in this section, an "issuer" is a company that is registered with the SEC in order to have its stock freely traded among investors. Among the disaster recovery community, this section was read as imposing a duty upon management to preserve records. The following comment is a frequently found summary of this provision:

> The section of this Act which keeps it at the forefront of disaster recovery liability is the "Standard of Care" wording, whereby management can be judged on their mismanagement of corporate assets.
>
> The FCPA is unique in that it holds corporate managers personally liable for protecting corporate assets. Failure to comply with the FCPA exposes individuals and companies to the following:

Personal fines up to $10,000
Corporate fines up to $1,000,000
Prison terms up to five years

See http://www.drj.com/new2dr/model/schr.htm.

I have been unable to find any regulation or case that actually provides legal backup to the portion of this statement that claims that there is civil or criminal liability for failure to have a disaster recovery plan to protect corporate assets. I think other laws and regulations provide a stronger argument that a publicly traded company needs to have at least some disaster recovery planning. However, I cannot categorically rule out the potential of someone being able to craft a course of action based solely on the FCPA. Because the cost of compliance is low and the potential risk (including personal risk) is high, the prudent public company board and management would adopt a disaster recovery/business resumption plan.

Internal Revenue Service — Taxpayers with Over $10 Million in Assets

It will not surprise any reader to learn that the law requires you to keep records that back up your tax forms. The tax code, Section 6001, allows the Internal Revenue Service (IRS) to define what constitutes a "record." Although many disaster-recovery Web sites will point you to IRS Procedure 86-19, that provision has been effectively superceded by IRS Revenue Procedure 98-25. I've included the multi-page text of that Procedure as "Appendix B."

Most of you will be happy to know that this procedure does *not* apply to all taxpayers. It only applies if the taxpayer keeps its records in machine-readable format, and the taxpayer has over $10 million in assets in the taxable year. (There are other requirements for insurance companies, companies where machine-sensible records were used for computations that cannot be reasonably verified or recomputed without using a computer, and corporations with foreign ownership. If your company belongs to one of those types, you will want to seek assistance from specialized tax counsel.)

If the rule *does* apply to your company, you must maintain documentation for the machine-readable system, label and store the records in a secure environment, and retain the ability to access the records. You must retain such records for at least seven years, with longer retention periods for records that relate to long-lived items.

One of the kickers in the rule is that you have to maintain the ability to recover records even if you've changed to a new system. For example, some of the older readers of this book will remember a word processing program called MultiMate. Back at the dawn of computers, we thought it was a whiz-bang application. We stored documents created in MultiMate on big 5¼-inch floppies that could actually

bend (thus, the name floppies). While it is an extreme example, if key tax information were kept on those floppies in MultiMate, this rule would require the ability to retrieve those records. This would also apply in the case of a merger or acquisition. For example, even if the acquiring company is (and always has been) a supporter of Apple software and hardware, it must retain the ability to retrieve records from an acquired company that believed in Windows.

From my perspective, the real disaster-recovery part of this rule comes from the first parts of Section 8 of the Procedure, which requires that

.01 Except as provided in section 9.02 of this revenue procedure, the taxpayer must promptly notify its District Director if any machine-sensible records are lost, stolen, destroyed, damaged, or otherwise no longer capable of being processed (as defined in section 4.02 of this revenue procedure), or are found to be incomplete or materially inaccurate (affected records).

.02 The taxpayer's notice must identify the affected records and include a plan that describes how, and in what timeframe, the taxpayer proposes to replace or restore the affected records in a way that assures that they will be capable of being processed. The plan must demonstrate that all of the requirements of this revenue procedure will continue to be met with respect to the affected records.

In other words, if a storm were to come along and destroy or damage your ability to retrieve some tax-related records, you must notify your local IRS office *and* tell that office how you're going to "replace or restore" the affected records. Experts in this area say that a failure to report known issues can lead to an "acrimonious relationship" with the IRS. For those companies with a good computerized backup program and a good disaster recovery plan, there should not be a problem complying with this requirement.

Your local IRS office can also periodically "test" your system to establish the authenticity, readability, completeness, and integrity of your records.

The lawyer in me does want to point out that there is such a thing as retaining too much information. I believe that all companies should have a document retention policy under which they can dispose of material that is no longer useful. It is far too easy to just say "keep it all," especially in this day of cheap gigabyte hard drives. However, if you ever get into a lawsuit, your opponent may be able to ask you to produce all your old records even if it would cost you thousands of dollars to retrieve and reproduce such records. As I have in other places in this chapter, I recommend that you consult with counsel to produce a document retention policy that makes sure that you keep what you need, but no more.

Food and Drugs — Contingency Recall Plan

If your company produces consumer products regulated by the Food and Drug Administration (FDA), you are required by federal regulations to have a contingency plan for a recall of such products. The FDA is the federal agency responsible for ensuring that foods are safe, wholesome, and sanitary; human and veterinary drugs, biological products, and medical devices are safe and effective; cosmetics are safe; and electronic products that emit radiation are safe. The complete set of recall procedures prescribed by FDA regulations can be found at http://ecfr.gpoaccess.gov. The portion of the rules that deals with contingency planning is 29 CFR 7.59, which provides in part:

> A recall can be disruptive of a firm's operation and business, but there are several steps a prudent firm can take in advance to minimize this disruptive effect.

Notwithstanding similar specific requirements for certain products in other parts of this chapter, the following is provided by the FDA as guidance for a firm's consideration:

> (a) Prepare and maintain a current written contingency plan for use in initiating and effecting a recall in accordance with §§7.40 through 7.49, 7.53, and 7.55.

While the alert reader will note that these are said to be "guidelines" for a firm's "consideration," it should also be noted that they are guidelines that the FDA thinks a "prudent firm" should follow. As a non-expert in this area, I read this as more than a gentle nudge to have such contingency plans; failure to have such a plan would brand the firm as "imprudent." I do not know all of the legal consequences of such a branding, but I feel confident that there are plaintiff-oriented law firms that would.

"Financial Institutions" — Gramm–Leach–Bliley (GLB)

Federal law requires that "financial institutions" must be sure to maintain the privacy of any private information that they hold. Act 15 USC 1508 provides the basis of this obligation:

Sec. 6801. Protection of nonpublic personal information

(a) Privacy obligation policy

It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to

protect the security and confidentiality of those customers' nonpublic personal information.

(b) Financial institutions safeguards

In furtherance of the policy in subsection (a) of this section, each agency or authority described in section 6805(a) of this title shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards —

(1) To insure the security and confidentiality of customer records and information
(2) To protect against any anticipated threats or hazards to the security or integrity of such records
(3) To protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer

Under GLB, a "financial institution" includes traditional institutions such as banks, credit unions, and securities brokers. It also covers other entities such as retailers that issue their own credit cards, real estate appraisers, insurance companies, automobile leasing companies, career counselors that advise applicants for financial organization openings, businesses that print and sell checks, tax preparation companies, companies that operate as travel agencies in connection with financial services, real estate settlement services, mortgage brokers, investment advisory companies, and credit counseling services.

The Federal Trade Commission (FTC) has adopted a set of regulations for financial institutions that are outside the scope of other federal agencies. The rule codifies the elements of a security plan for such firms and can be found at 16 CFR 314.4:

§ 314.4 Elements

In order to develop, implement, and maintain your information security program, you shall:

(a) Designate an employee or employees to coordinate your information security program.
(b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:
    (1) Employee training and management
    (2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal
    (3) Detecting, preventing and responding to attacks, intrusions, or other systems failures

(c) Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures
(d) Oversee service providers, by:
  (1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue
  (2) Requiring your service providers by contract to implement and maintain such safeguards
(e) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.

As a result of GLB, multiple agencies with jurisdiction over more traditional "financial institutions," such as banks, and savings and loans, adopted "Interagency Guidelines Establishing Standards for Safeguarding Customer Information." A copy of those guidelines can be found at http://www.complianceheadquarters.com/AML/AML_Research/66FR8615.txt. The language of the regulations for each financial institution is the same. For example, the regulations that apply to banks are included at the end of this chapter as Appendix C.

Even though the rules that apply to banks and other formal financial institutions such as savings and loans and credit unions are more detailed than those that apply to a car leasing company, the basic objectives are the same: (1) have a responsible officer in charge, (2) do a risk assessment, (3) prepare and implement a plan, (4) oversee service providers, and (5) adjust the plan as needed in light of changes. The other parts of this book provide you guidance on how to do this for financial information and corporate information.

Preparedness Planning Is Encouraged by Law

This section of this chapter brings to your attention laws, rules, and regulations that *encourage*, but do not *mandate*, disaster recovery planning. The importance of these statutes and rules is that it is a very easy step for a government agency or a court to say that any entity that does not follow such "encouragement" is imprudent. It is also easy for such encouragement to become part of regulations that are effectively mandated — even if not expressed in such terms.

Intelligence Reform and Terrorism Prevention Act of 2004 — NFPA 1600

As 2004 was coming to a close, Congress passed, and the President signed, the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108-458). A portion of that law dealt with encouraging the private sector to do its own preparedness planning:

SEC. 7305. PRIVATE SECTOR PREPAREDNESS

(a) FINDINGS — Consistent with the report of the National Commission on Terrorist Attacks Upon the United States, Congress makes the following findings:
  (1) Private sector organizations own 85 percent of the Nation's critical infrastructure and employ the vast majority of the Nation's workers.
  (2) Preparedness in the private sector and public sector for rescue, restart and recovery of operations should include, as appropriate —
    (A) A plan for evacuation
    (B) Adequate communications capabilities
    (C) A plan for continuity of operations
  (3) The American National Standards Institute recommends a voluntary national preparedness standard for the private sector based on the existing American National Standard on Disaster/Emergency Management and Business Continuity Programs (NFPA 1600), with appropriate modifications. This standard establishes a common set of criteria and terminology for preparedness, disaster management, emergency management, and business continuity programs.
  (4) The mandate of the Department of Homeland Security extends to working with the private sector, as well as government entities.

(b) SENSE OF CONGRESS ON PRIVATE SECTOR PREPAREDNESS — It is the sense of Congress that the Secretary of Homeland Security should promote, where appropriate, the adoption of voluntary national preparedness standards such as the private sector preparedness standard developed by the American National Standards Institute and based on the National Fire Protection Association 1600 Standard on Disaster/Emergency Management and Business Continuity Programs.

I will be the first to tell you that this "law" has no force and effect in and of itself. It only suggests that the Secretary of Homeland Security "should promote" standards, but only when they are "appropriate" and "voluntary." The NFPA is not the only standard the Secretary can promote, but it is the only one specified by name.

However, I will also tell you that I am not aware of any *other* set of preparedness standards that has such a federal-law "blessing." Thus, if I were designing a disaster recovery plan to comply with some *other* federal law or regulation, I would look to NFPA 1600 as a useful template. Compliance with NFPA 1600 would become

what is known in the law as a "safe harbor" — a standard that if complied with, is deemed to satisfy a rule or regulation.

Stated another way, why *wouldn't* a company follow NFPA 1600? It has been endorsed by federal law, is the product of the same kind of standard-making that gives us many other codes and standards, and is designed to be flexible and adapt to any organization. Wouldn't it be prudent business practice for the company to follow this standard? If questioned as to its disaster recovery planning, following this standard would show how smart and prudent the management of the company was.

The NFPA is somewhat poorly named because it is an international — not national — body with over 60,000 members from all over the world, and members associated with fire departments make up only about a quarter of its membership. It develops standards through a consensus process that is approved by the ANSI. The NFPA standards are routinely adopted by state and local lawmakers for building, life safety, and electrical standards.

The 2004 Standards relating to disaster recovery can be found at http://www.nfpa.org/assets/files/PDF/NFPA1600.pdf. You should not be intimidated by the 46-page size of the document. The actual Standards themselves are contained on pages 1600–4 through 1600–7. Those four pages of Standards are then followed by several pages of "explanatory material," which contain much of the meat of the standards. The Standards are written in "shall" language, indicating that following them is mandatory, whereas most of the explanatory material is written in "should" language, indicating concepts that are just advisory in nature. While the Standards are written in terms of the duties of an "entity," the summary presented in the following text speaks of a "company," as that is the main target of this book.

The Standards begin with principles of **Program Management**. These standards state that a company shall have a documented program that sets out the executive policy of the company, including vision, mission statement and enabling authority; goals and objectives; plans and procedures; applicable laws or regulations; and the budget, schedule, and milestones of the project. One "program coordinator" is given the authority to administer and update the project. If the company uses advisory committees, an advisory committee shall assist the program coordinator in the creation of the plan. The plan should be periodically evaluated.

With regard to the specific **Program Elements**, the Standards call for plans that deal with the four phases of disaster/emergency management: mitigation, preparedness, response, and recovery. The first objective of the plan is to comply with "applicable legislation, regulation, directives, policies and industry codes of practice." See Standard 5.2.1.

The process begins with a risk assessment, in which the company identifies hazards, determines the likelihood of their occurrence, and the vulnerability of the enterprise to those hazards. Although the "explanatory materials" list numerous types of hazards, the Standards themselves break them down into two categories — natural and "human caused."

As part of the risk assessment, the Standards call for an impact analysis. The purpose of the impact analysis is to determine the potential for harm to the company from the identified hazards. The potential impacts to be considered include the health and safety of the persons in the affected area and those persons that respond to the incident; the impact of the incident on continuity of operations; the property, facility, and infrastructure; the delivery of services, the environment, economic and financial conditions of the company, regulatory and contractual obligations; and the reputation of and confidence in the company.

The Standards then call for **Hazard Mitigation**, taking into account the risk assessment and impact analysis and a cost–benefit analysis. In order to mitigate the hazard's risk, the company should consider: the use of building construction standards; land-use practices; relocation, retrofitting, or removal of structures at risk; removal or elimination of the hazard; reduction or limitation of the amount or size of the hazard; segregation of the hazard; modification of the basic characteristics of the hazard; control of the rate of release of the hazard; protective systems or equipment for both cyber and physical risks; establishment of hazard warning and communication procedures; and redundancy or duplication of essential personnel, critical systems, equipment, information, operations, or materials.

The Standards call for **Resource Management**. Without summarizing this area too much, it essentially calls for the coordinator to figure out what the company has as far as resources go, what additional resources are needed, and how to close the gap between the two. The Standards also call for **Mutual Aid** agreements between the company and other possible suppliers.

- Planning is one of the core recommendations of the Standards. The Standards call for five types of plans:
  - Strategic — Defines the vision, mission, goals, and objectives of the program
  - Emergency Operations/Response — Sets forth responsibilities of individuals and organizations to carry out specific actions in event of an emergency or disaster
  - Mitigation — As the title indicates, the plan to eliminate hazards or reduce the impact of those hazards on the company
  - Recovery — Provides for strategy, priorities, and time frame for restoration of services, facilities, programs, and infrastructure
  - Continuity — Identifies the critical and time-sensitive applications, vital records, processes, and functions that must be maintained, including the personnel and procedures necessary for the process

All of the plans should spell out the specific roles and responsibilities of the participants in the plan and specify the lines of authority to be followed by the plan. Each plan should state who is in charge in the event of an incident, and what policies they should follow in coordinating with outside authorities.

Key parts of good contingency planning are **Communication and Warning**. The Standards call for the establishment and periodic testing of such communications procedures. Your people need to know when to call for help from emergency response personnel. You need to have the appropriate warning protocols for emergencies and train your people as to what to do when the alarms go off.

The Standards probably break the planning process down into more parts than is practical in most organizations. For example, it says that all organizations should have **Operations and Procedures** to support the plans. One such procedure is a "situational analysis" that includes damage assessment and the identification of resources needed to respond to the incident. Another recommended procedure is the establishment of a succession of management authority in the continuity plan. The company should also have the **Logistics and Facilities** to implement the plan, including necessary emergency equipment and personnel and, when appropriate, an alternate facility capable of supporting operations during the incident.

Naturally, **Training** is a component of the planning process. The company is directed to assess its training needs and develop and implement the appropriate training curriculum. Management should determine the "frequency and scope" of training, and records of training should be maintained.

Once the employees have been trained in the plans, they should undergo **Exercises, Evaluations, and Corrective Actions**. In other words, the plans should be tested — either individual elements of the plan or the entire plan. If any deficiencies are identified, corrective action should be taken.

A sometimes-overlooked element of a good plan is the **Crisis Communication and Public Information**. Companies should develop procedures for providing information before, during, and after an incident, including information for both employees and the media. The Standards include a central contact facility for the media, a disaster/emergency information handling system, and prepared information bulletins. A company should have a method to determine what information is released, when it is released, and what steps are necessary for clearance for the release. The company should also think about communications with a special-needs population, for example, the hearing impaired or the sight impaired. Finally, the company should consider whether it would recommend seeking shelter or evacuation for various types of incidents.

Of course, no plan can be effective without **Finance and Administration**. The Standard (5.15.1) in this regard is clear: "The entity shall develop financial and administrative procedures to support the program before, during and after an emergency or disaster." In this regard, the Standards encourage swift decision-making on fiscal questions and defined responsibilities for the program's financial authority.

The reader will recognize that I have spent several pages summarizing the Standards, even though they are nominally voluntary in nature. I have done so because of their impact on numerous other disaster recovery or continuity of operations planning documents. In doing research on this chapter, I have seen

numerous references indicating a particular plan was devised, at least in part, in compliance with the Standards. The basic elements outlined by the Standards — an impact analysis, a gap analysis, planning, testing, communications, and finance — are the basic elements of every comprehensive disaster recovery plan. If your company adopts no other plan, it should consider and follow NFPA 1600.

Pandemic Planning

As I was working on this chapter, the federal government released a new document titled *National Strategy for Pandemic Influenza Implementation Plan.* The full document can be found at http://www.whitehouse.gov/homeland/nspi_implementation.pdf.

The primary focus of the plan is on the federal response — what federal agency will have what authority, how the borders will be monitored, how human health will be protected, etc. However, it also recognizes that the government will not be alone in responding to such a pandemic, and calls on businesses to establish their own plans. In a severe pandemic, up to 40 percent of the workforce could be off the job for two weeks, the report estimates. Because 85 percent of the systems that are vital to society — food production, medicine and financial services — are privately run, the administration aimed to use the new report to energize businesses in particular to start planning how they will keep running under those conditions.

In that regard, the government has prepared a "checklist" for business. The checklist is included as "Attachment D" and is taken from http://www.pandemicflu.gov/plan/businesschecklist.html.

Public Companies — Sarbanes–Oxley and SEC Rules

There is another chapter of this book dedicated to the impact of Sarbanes–Oxley on disaster recovery planning, so I will not duplicate the work of that chapter. However, I will give "the law" on the topic and leave it to Dave to give you the accountant's perspective on the law.

Sarbanes–Oxley

Sarbanes–Oxley arose out of accounting scandals, mainly Enron and Worldcom. Key provisions of Sarbanes–Oxley (codified at 28 USC 1658b, *et seq.*) include

- Section 302, which requires that a public company's financial statements be certified by the Chief Executive Officer and the Chief Financial Officer

- Section 404, discussed in detail in the following text
- Section 409, which requires companies to promptly disclose material changes to their financial conditions or operations
- Section 1106, which increases penalties for violation of the law

With regard to disaster recovery planning, most authorities point to Section 404 of the Act, which provides for the following:

Section 404: Management Assessment of Internal Controls

(a) RULES REQUIRED — The Commission shall prescribe rules requiring each annual report required by section 13 of the Securities Exchange Act of 1934 (15 U.S.C. 78m) to contain an internal control report, which shall —
   (1) State the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting
   (2) Contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

(b) INTERNAL CONTROL EVALUATION AND REPORTING — With respect to the internal control assessment required by subsection (a), each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagements issued or adopted by the Board. Any such attestation shall not be the subject of a separate engagement.

The Sarbanes–Oxley Act created the Public Company Accounting Oversight Board (PCAOB), which is charged with drafting rules for auditors and accountants. On March 9, 2004, the Board released standards regarding safeguarding of assets. The Board determined that "management's plans that could potentially affect financial reporting in future periods are not controls." It concluded that "a company's business continuity or business planning is not part of internal controls over financial reporting." — PCAOB Release 2004-001, Page A-135.

Some parties have argued that the decision by the Board puts an end to the argument that Sarbanes–Oxley requires disaster recovery planning. I think that is an over-reading of this particular provision. Other portions of Sarbanes–Oxley require retention of audit records by the auditors and forbid the destruction of such records for a period of time. I believe it is totally consistent with the intent of Sarbanes–Oxley that a company have a plan to safeguard all of its assets, including all the information used for the preparation of its public reports.

SEC Rules

On November 3, 2004, the Securities and Exchange Commission (SEC) approved the final corporate governance rules established by the New York Exchange (NYSE) known as Section 303A, and the NASDAQ known as SR-NASD-2002-141. These rules apply to all of the companies that are traded on either the NYSE or the NASDAQ. Although the new rules are not identical for both bodies, they are similar with regard to the topic covered by this chapter. These new sections encompass all risks facing an organization — hazard, financial, operational, and strategic. For example, the rules require corporate boards and management to improve their processes and policies for risk assessment and management. They also contain requirements associated with audit committees, corporate codes of conduct, and director and board independence. The complete NASDAQ rules are posted at http://www.nasdaq.com/about/CorporateGovernance.pdf. The NYSE rules are posted as part of the "Listed Company Manual" at http://www.nyse.com/Frameset.html?nyseref=&displayPage=/listed/1022221393251.html.

The rules require the company's audit committee to "discuss policies with respect to risk assessment and risk management." The commentary to the rule requires the audit committee to "discuss the listed company's major financial risk exposures and steps management has taken to monitor and control such exposures."

It is clear that the primary focus of these rules is on the type of financial risk exemplified by the Enrons and WorldComs of the world. However, "risk" goes beyond just the financial, and should include anything else that could adversely affect the way a company does business — for example, the impact of a natural disaster. Although I cannot currently point to any specific legal authority that includes this definition of "risk," I believe the prudent audit committee would be wise to examine the company's business continuity plans as a part of a comprehensive examination of risk. Once again, I believe that compliance with NFPA 1600 would demonstrate the kind of risk mitigation that is appropriate for a public company.

ISO Certification

As the information industry started to mature, security quickly became a concern. Everyone now knows that hackers and viruses can compromise a computer system. Although it is possible to produce a fairly secure internal system, every computer system also relies on outside vendors. How can a company know that its *vendors* and business partners also have high standards of computer security? The industry's answer, by way of the International Standards Organization (ISO), was to devise what is now ISO 17799:2005. Many companies will at least be familiar with the terms of ISO 9000 (which deals with quality management) or ISO 14000 (which deals with environmental management) compliance. ISO 17799 is just the standard that deals with information security and the ":2005" portion indicates that it

was revised in 2005. (ISO 17799:2005 will be renamed to ISO/IEC 27002 in the future.) All of the ISO standards are voluntary.

ISO 17799:2005 is a complex and detailed international information security standard. Compliance and certification enables companies to show their business partners and customers that they have met a high standard of security. The requirements, which are programmatic in nature, cover 11 core areas: security policy, security organization, asset management, personnel security, physical security, communications and operations management, access control, information systems acquisition and development, information security incident management, compliance, and — of interest for this chapter — business continuity management.

Achieving ISO 17799:2005 certification could give your company a competitive advantage over a company that does not have such a certification. Which would your customers rather deal with — a company that can demonstrate that it meets the highest standards of information security, or one that does not have such documentation?

It appears that the ISO 17799 standard is proprietary. I have not been able to find the actual text of the document on the Web. With regard to the business continuity portion of the standard, one Web site (http://praxiom.com/iso-17799-2005.htm) listed the following breakdown of steps:

14.1.1 Establish a business continuity process for information.
14.1.2 Identify the events that could interrupt your business.
14.1.3 Develop and implement your business continuity plans.
14.1.4 Establish a business continuity planning framework.
14.1.5 Test and update your business continuity plans.

A company that is interested in achieving certification for its compliance with ISO 17799:2005 should either purchase the entire standard from the ISO at http://www.iso.org/iso/en/prods-services/popstds/informationsecurity.html or seek a consultant with ISO 17799 experience.

Radio, Television, Cable, and Satellite Broadcasters

The FCC has created a federal advisory committee called the Media Security and Reliability Council (MSRC). The MSRC is "designed to assure the optimal reliability, robustness and security of the broadcast and multi-channel video programming distribution industries in emergency situations." In March, 2004, the MSRC provided the FCC with a set of comprehensive "best practice" recommendations. The complete text of those recommendations can be found listed as "Model Disaster Recovery Plans" at http://www.mediasecurity.org/documents/index.html.

That site lists separate plans for Local Cable Systems, Direct Broadcast Satellite, Local Radio Stations, and Local Television Stations.

The model plans emphasize that they are voluntary in nature. Although it is possible that the FCC will someday make such plans mandatory, that date may be far in the future.

Although the industry-specific plans vary in some instances, their basic content is familiar — establish a disaster recovery group, do a risk assessment, prepare a plan, test the plan, and continue to improve the plan. The plans emphasize the establishment of backup generators, backup broadcast facilities, and the execution of cooperation agreements between providers in an area. Broadcasters are also encouraged to have alternate forms of communication, so that if one system goes out, others can be used. For example, one recommendation is to have a "ham" radio station available to the broadcast facility in the event that other forms of communications are not available. If your company is in the broadcast industry, it should investigate and implement the recommended disaster recovery plans.

General Risk Management

It is difficult to imagine a company in America that does not carry some form of insurance. Usually, the company will have several types of insurance, depending on the different types of risk. One way that companies can keep their insurance rates low is by demonstrating safe operating procedures. A good disaster recovery plan can be part of a comprehensive approach to safety and risk reduction.

One of the leaders in corporate safety is the Walt Disney Company. As host to millions of visitors and the source of employment for thousands of "cast members," Disney has placed a high emphasis on safety. A comprehensive report on Disney safety measures can be found at adisneyland.disney.go.com/ media/ dlr/content/eng/safety/Safety_Report.pdf.

Of course, Disney has a disaster recovery program with some unique features.

The four hurricanes that struck Florida in summer 2004 caused millions of dollars in damage and disrupted countless lives. Although central Florida had not experienced a hurricane during the entire time Walt Disney World has operated (it opened in October 1971), the resort had in place a five-step plan for gradual curtailment of operations in case of a hurricane. As three of the four hurricanes interfered with Walt Disney World's operations, the resort's managers were able to put the plan into operation and use the lessons of the hurricanes to improve on it. The plan specified five phases of reduced operations, ranging from monitoring the storms to shutting down activities and moving workers to shelter. Key lessons of the experience were that working with local media was an effective way to distribute information; communication with employees and guests is essential; and it is worthwhile to provide guests with as much of a "resort experience" as possible even when they must remain in their rooms for safety's sake. In that last regard, the resort's entertainers moved to the hotels and continued to interact with guests when they could, and the resort recognized the importance of a hot meal

for guests who had been confined to their rooms (see http://www.allbusiness.com/periodicals/article/325473-1.html).

In other words, during the hurricane, it might have been possible to have a hot meal and a visit from Cinderella while staying at a Disney resort! Now *that's* fancy planning!

I have heard a story about Disney's response plan if an accident occurs in one of its parks. I have not been able to find my source, so this may be a lawyer's urban myth. (If you can confirm — or deny — this report, please send me a note at empope@tellawcomlabs.com.) At any rate, the story goes that every cast member is trained to take the injured party and his or her family to a designated "backstage" area. Any injuries that can be treated on the spot are taken care of while the family is on Disney property. Disney counselors meet with the family while the loved one is being taken care of. A park official apologizes to the family and offers tokens of condolence — for example, lifetime passes to the park. The official also strives to have the family sign a release prior to leaving park property. This coordinated response has meant that Disney has managed to keep its liability levels much lower than that of other similar theme parks.

The other part of the Disney legend, which I can demonstrate is untrue, is that Disney never loses a court case and never settles. I think the part of the legend that *is* true is that the Disney company lawyers will vigorously defend the company (and Disney will pay for enough lawyers for a strong defense) and that it is an uphill battle to prevail against Disney in one of the locations where it operates. Thus, I'm sure that only a few plaintiff law firms have the resources to go toe-to-toe with such a determined operation.

The point of all of this discussion is to get you to think — would it help your insurance rates if you were to install a Disney-level attention to safety? Would your employees and customers be safer? Would your company be able to bounce back more quickly from an accident? If the answer to any of these questions is "yes," then I believe you have a business reason for a comprehensive safety program, which includes a disaster recovery plan.

Contract Obligation

Your company may have an obligation to perform its duties under contract even if the contract has a *force majeure* clause. The phrase literally means "greater force." These clauses excuse a party from liability if some unforeseen event beyond the control of that party prevents it from performing its obligations under the contract. Typically, *force majeure* clauses cover natural disasters or other "Acts of God," war, or the failure of third parties — such as suppliers and subcontractors — to perform their obligations to the contracting party. It is important to remember that *force majeure* clauses are intended to excuse a party only if the failure to perform could not be avoided by the exercise of due care by that party.

One typical example of a force majeure clause reads:

> If the performance of this Agreement is interfered with by reason of any circumstance beyond the reasonable control of the Party affected as a result of fire, flood, explosion, war, strike, embargo, government requirement, civil or military authority, act of nature or the public enemy, or act or omission of carriers (each a "Force Majeure"), then the Party affected shall be excused from such performance on a day-for-day basis to the extent of such interference, provided the Party so affected shall use commercially reasonable efforts to remove such causes of non-performance.

It used to be that *force majeure* clauses were just part of the "boilerplate" of a contract, and the parties did not spend a lot of time working on them. Because of the developments of 9/11 and Katrina, these provisions have become much more important.

For example, let's say that your contract is to deliver 100 widgets a day to your customer, except as provided in the clause just outlined. After the contract is signed, the United States invades Iraq. The war in Iraq causes the price of widgets to go up 10 percent. Can your company stop delivery because of the war? I think most courts would say "no," and require your company to continue to provide all 100 widgets at the agreed-upon price.

Now, let's say the bird flu causes about half of your workforce to get sick. Your production line can no longer supply all the contracted widgets to every customer. You impose a rationing, delivering to each customer a proportional amount of widgets. Would your company be able to stop delivery completely because of the flu? Possibly. Could one or more of your customers sue you, despite the *force majeure* clause? You bet.

I could go on, but you get the message — *force majeure* clauses may not exempt your company from performance even in the event of a disaster or emergency. Although I can't provide you with a case on point, I believe a court would take into account your efforts to comply with the contract despite the disaster and would also consider whether or not you had taken reasonable steps to mitigate the impact of the disaster. In other words, a good disaster recovery plan might help your legal status in the event of a lawsuit.

While I'm talking about *force majeure* clauses — is there a supplier that *your* company needs to be able to deliver, regardless of circumstances? You might want to look at renegotiating your *force majeure* clause with that company to make it clear under which circumstances that company would be allowed to stop providing you with goods or services.

Crisis Management

Last night, while watching TV, I saw the Bausch & Lomb CEO announce a full recall of a certain contact lens solution, with a recommendation that users use

another product produced by the company. I don't know anything about the particular crisis that is currently afflicting Bausch & Lomb; I did recognize the elements of one of the best crisis management ever — the way Johnson & Johnson handled the Tylenol scare.

Early in the 1980s, people in Chicago were dying from a mysterious cause. The police finally determined that someone was placing cyanide in Tylenol capsules and placing the capsules back on store shelves. It was fairly clear that the tampering was occurring outside of the Johnson & Johnson plant, and that the poisonings were confined to the Chicago area. Johnson & Johnson could have legitimately tried to downplay the reaction and tried to "spin control" the problem.

However, they took an alternate tack. They pulled *every* Tylenol capsule from the market and put the Johnson & Johnson CEO out in front of the publicity campaign — explaining that the customers' health and safety were of primary concern. A few weeks later, Johnson & Johnson brought out new tamper-resistant packaging, again with a major publicity campaign. Although the company suffered an initial loss, the final result was actually positive — sales resumed their previous levels and customers reported that they had high opinions of Johnson & Johnson. Ever since that time, the Tylenol approach has been the "gold standard" against which all other crises have been measured.

You may think that your product is unlikely to be the subject of a health scare. However, it is possible for just about *anything* used by the consuming public to be suddenly tainted. Older readers will remember when it was rumored that cell phones caused brain cancer. It did not matter that millions of people had been using cell phones for years and that there was no statistical correlation between such phones and cancer. The rumor was widespread and caused instant concern for cellular companies. In retrospect, the industry should have been prepared — but it wasn't. It had to play catch-up by forming a blue-ribbon panel to look into the allegations and then promote the results of that panel's study. (It should be noted that what was bad for the cell phone industry was good for a few promoters of "protection devices" that were supposed to keep the user safe from cancer. The fast-moving entrepreneurs of that industry identified an immediate need and met it.)

In other words, it is time for *your* company to have a plan for what your response would be if there were some kind of health scare associated with your product. The plan should follow the Tylenol pattern — a prominent member of management, a widespread recall, a single message, and a well-publicized rework of the product to respond to the threat. You should determine now who the spokesperson should be, plan on who is responsible to produce the message, and determine the process by which the message will be developed and released.

Other

Some commentators on disaster recovery plans have argued that there may be some kind of shareholder action if a board were to fail to adopt a disaster recovery plan. The "legal" theory presented states that directors have a responsibility to be prudent stewards of corporate assets, and that failure to have a disaster recovery plan would be a breach of that duty. If such a firm were to experience a catastrophe and not recover from it as swiftly as other, prepared, firms, the theory holds that the shareholders would be able to hold the board liable for such inaction.

I think each element of the theory has potential merit. I certainly cannot say that such a lawsuit could not be brought or would be successful if brought. However, I am somewhat cautious about this claim. I have not seen a case that adopts this theory, and until there is legal precedent, I'm not going to tell my corporate clients that disaster recovery planning is *mandated* by this theory. A risk-adverse board of directors should adopt a disaster recovery plan because it is the prudent thing to do.

I also think it would be fairly easy to start a shareholder call to action to insure that all publicly held companies have disaster recovery plans. As noted previously, NYSE and NASDAQ firms must consider risk management in order to comply with corporate governance rules. I think that a shareholder rights group like the California Teacher's Pension Fund could insist that every firm in which they invested have a disaster recovery plan and could sponsor shareholder resolutions at the annual meeting to compel such plans.

Preparedness Planning for the Legal Department

If you are a lawyer and reading this, in all probability it is because someone else in your company (or one of your clients) has provided it to you with a request that you evaluate whether the law requires them to produce and adopt a disaster recovery plan. You will see that I've tried to make the process easy for you by providing the citation to the statute or rule involved and, in most cases, provided the actual text of the statute or rule. With those tools, I hope you will be able to give your client the necessary guidance about companywide disaster recovery planning. However, your task should not end there. You should also evaluate your responsibility to your company or client to have a disaster recovery plan that is specific to the legal function.

I can't point to a section of the Code of Professional Responsibility or the Disciplinary Rules as an authority that says that lawyers should prepare their own disaster recovery plans. However, I think most of you, if you review this chapter, will recognize that there are steps that *should* be taken even if you are not required to take them. (If you read other parts of this chapter, you will see that, except for a few highly regulated industries, most companies are in the "should" but not "must" category. I hope you use this opportunity to encourage your company or client to adopt a planning process as a part of prudent management.)

Your disaster recovery plan does not have to be elaborate or expensive. However, it should require you to plan for the most common types of disaster. For example, how would your department react if a Katrina hit your city and you couldn't even get to your office for several weeks? How would you respond?

Document Protection

When I was the in-house General Counsel of an entrepreneurial telephone company, I insisted that the Legal Department be the keeper of *all* the original contracts to which the company was a signatory. I had all the original contracts stored in one of those vault-like filing cabinets — the ones that are supposed to be fire resistant and super safe. At the time, I thought that was enough protection for the company.

I now realize that the level of protection afforded by those filing cabinets was illusory. If a Katrina-like catastrophe had hit, I wouldn't have been able to *get* to those cabinets or the files that they contained. Assuming an evacuation of the city, I would have needed remote access to those files and would not have been able (at that time) to get to them.

Of course, you have it easier. My General Counsel days were also the days prior to PDFs and other electronic storage media. However, it also means that there is little excuse for you not to have a full set of key documents backed up and placed where they can be remotely retrieved. You should establish a routine that every key company document be imaged immediately after signature and stored in a remote location. If your company is large enough, your computer gurus — whether now called IT, MIS, or something else — should already have a remote-site backup system in place. You can work with them to identify the key documents and determine how and where the documents are to be stored and retrieved.

If, however, you don't have a bunch of computer experts at your disposal, you should still set up a backup site of your own. The easiest such location would be a branch office of your company. Make an image of each important document and ship it to that location. If you don't have a branch office, use one of your outside law firms that is distant from your office. They will be delighted to be your repository and probably won't even charge anything for the service. Just be sure to let the partner that you work with most know that they are your emergency backup repository, so that the partner can keep your files in a safe place. (Of course, this is your opportunity to find out if your outside law firm has a disaster recovery plan of its own. It won't do you any good to back up data and suddenly find out that the firm can't find it.)

There are also commercial firms that specialize in keeping backup data. An Extranet, such as West's WorkSpace, lets attorneys access client case information, calendaring programs, client data, and billing from a server that is located off-site. Whether working at the office, at home, or in temporary quarters, all the data remains accessible. Companies with names such as LiveVault, eVault, and

AccessGenie are all vying for the Web-based backup market share. For a firm of any size it makes sense to take a look at what these and similar companies have to offer. That can give your firm peace of mind.

As noted above, some providers also allow you to keep data such as court calendars and filing deadlines on their servers. I'll admit that, traditionally, I've kept all of that information in a very old-fashioned way — written on my calendar at work. With that calendar, I knew what was due and when it had to be filed. However, if something were to happen where I couldn't *get* to that calendar, I would have been helpless. I know many of you have already solved that problem by putting your calendar on your computer or Blackberry. However you want to do it, it is important that you establish a system that you can access away from your office that will tell you when documents need to be filed. It's very easy to establish such a system when the sky is sunny and everything is fine; it's almost impossible to do in the middle of a major catastrophe.

While we're thinking about important documents, please take a moment to think about what is important to your vendors as well. If you're like most in-house law departments, one of your largest expenses is outside counsel. On behalf of all the outside counsel of the world, I ask that you treat our bills as important documents that should be stored and recovered in the event of a crisis. Of course, most law firms would be able to redo the bill for you, but would greatly appreciate it if you were able to continue to pay your bills during times of crisis. (Note to law firms: Your billing system is your cash register. You are being penny wise and pound foolish if you don't have a backup system for your billing records.)

Backup Office

This is probably also a good moment to consider where you would go if your department had to evacuate your office and be gone for a while. If, for example, your office is in New Orleans, your contingency plan might be to go to Baton Rouge. (I'm assuming that there is no corporate contingent office.) If you do have a place in mind, it makes sense to document where it's going to be, what space will be available, what communications capabilities will be provided, etc. Will there be desks and office equipment available? Do your secretaries and paralegals know that such a space exists and how to get there? (Once again, think about one of your out-of-town outside law firms as a potential resource. I know my former firm made major efforts on our clients' behalf after Katrina hit New Orleans. You might have a lot of emergency options if you think about them ahead of time.)

The Law Library

Many companies, and virtually every law office of significant size, will have a law library. If you have an in-house law librarian, disaster recovery planning for the

library should be part of his or her job responsibility. If you don't have such a librarian, then it is the responsibility of the head of the legal department to make plans for the protection and replacement of the library. The chief danger to a library is water. A well-designed library keeps the books away from potential leaks. There are recovery methods if a single book is damaged. If a large number of books are damaged, you will want to consult with a professional. You need to know, in advance, who that professional is and what services he or she can offer.

Call-Out Lists

Once again, let's suppose that your headquarters has been hit by Katrina. Luckily, you've evacuated and are now safe in Baton Rouge. Do you have a list of people who need to be called immediately? Outside counsel? Clients? Vendors? How about e-mail addresses?

Once again, this list does not need to be elaborate. It can be as simple as a printed call-out list that you keep at home or in your briefcase. If you have a backup vendor, your vendor should also be able to store this information for you. A few moments putting the list together now will be amply repaid should the list ever be needed.

Succession

What would happen if one of the key members of your legal team were hit by a bus this morning? After dealing with the immediate grief, would you know what projects he or she was working on? Do you have a routine system for allocating work so that there is always a backup lawyer that knows at least the basics of the case? Do you have an outside lawyer who might be able to take over?

Now, what happens if the person who is responsible for your disaster recovery plan is hit by that bus? Does everyone else know where the plan is? Is there someone who has the backup responsibility to execute the plan?

Testing, Training, Updating

There are complete sections of this book devoted to these topics, so I won't say much here. You should, of course, test your backup system from time to time. I'd suggest the Mondays related to Daylight Savings Time — in other words, the day after you "spring forward" or "fall back." It's already a day that folks are reminded to replace the batteries in their smoke detectors at home, so it should be an easy day to remember to use to test your disaster recovery plans.

You should also do an occasional full-scale test — schedule an "emergency test day" where everyone is required to show up at the alternate work site with only the materials that they keep at home or that can be recovered from the backup systems.

Pretend that the office is completely unavailable. What gets done well and what needs improving?

It is especially important for the legal department to keep its plan updated. What happens if your call-out list does not include the newly hired Chief Information Officer but includes a former disgruntled employee? For law firms, is your client call-out list current? It would be embarrassing to make a call at home to someone you thought was still an attorney with a client, only to find out that he now represents a major competitor.

Personal Recovery Plans

As a final note to the lawyer who should be reading this portion of this book — it may be wise for you to have your own personal recovery plan in case something disastrous were to happen to your company or firm. You might not think you need such a plan, but life has a way of throwing surprises our way. For example, think of all the Arthur Anderson employees who were totally unconnected to Enron, who suddenly found their company under investigation and finally dissolved. Several major law firms took major hits during that same debacle, and I'm sure more than one attorney suddenly found himself or herself on the street. What would you do?

Of course, the "ordinary" answer is that you'd start a new job search. You'd scan job sites, work your network, send out resumes — all the standard stuff. What I'm suggesting to you, however, is that you also have an alternate career — something that will at least pay some of the bills — during the period when you're "between assignments." If you have a hobby that can make you some money, be sure that you keep up your skills and networks in the area of that hobby with just as much diligence as you do with your law career. I hope that no one reading this ever *has* to use his or her emergency plan, but if I've helped one other lawyer successfully think about the issue of "What would I do if I couldn't practice law," I'll feel as though my effort was not in vain.

APPENDIX A: Best Practices

7-7-1001	Network operators, service providers, equipment suppliers, and property managers should formally document their business continuity processes in a business continuity plan covering critical business functions and business partnerships. Key areas for consideration include plan scope, responsibility, risk assessment, Business Impact Analysis (BIA), plan testing, training, and plan maintenance.
7-7-1002	Network operators, service providers, and equipment suppliers should consider establishing a business continuity executive steering committee (composed of executive managers and business process owners) to ensure executive support and oversight.
7-7-1004	Network operators, service providers, equipment suppliers, and property managers should review their Business Continuity Plans on an annual basis to ensure that plans are up to date, relevant to current objectives of the business, and can be executed as written.
7-7-1005	Network operators, service providers, and equipment suppliers should perform a BIA to assess the impact of the loss of critical operations, support systems, and applications.
7-6-1006	Network operators, service providers, and equipment suppliers should consider establishing a designated Emergency Operations Center. This center should contain tools for coordination of service restoration, including UPS, alternate means of communications, maps, and documented procedures to manage business interruptions and disasters.
7-6-1007	Network operators, service providers, and equipment suppliers should consider establishing a geographically diverse backup Emergency Operations Center.
7-7-1008	Network Operators, service providers, and equipment suppliers should use the Incident Command System Standard for incident coordination and control in the emergency operations center and at the incident site.
7-7-1009	Network operators, service providers, and equipment suppliers should regularly conduct exercises that test their Disaster Recovery Plans. Exercise scenarios should include natural and manmade disasters (e.g., hurricane, flood, nuclear, biological, and chemical).
7-7-1010	Network Operators, Service Providers and Equipment Suppliers should designate personnel responsible for maintaining Business Continuity and Disaster Recovery Plans.

7-7-1011	Network operators, service providers, equipment suppliers, and public safety authorities should establish alternative methods of communication for critical personnel.
7-6-1013	Network operators, service providers, and equipment suppliers should review their insurance requirements to maintain business continuity in the event of massive property damage or loss, incapacitation of senior officers, and other interruptive situations.
7-7-1015	Network operators and service providers should make available to the disaster recovery team "as-built" drawings of network sites.
7-6-1016	Network operators and service providers should develop processes or plans to quickly account for all employees (e.g., field techs) in or near the impact area of a disaster.
7-6-1017	Network operators and service providers should have documented plans or processes to assess damage to network elements, outside plant, facility infrastructure, etc., for implementation immediately following a disaster.

APPENDIX B: IRS Rev. Procedure 98-25

Section 1. Purpose

The purpose of this revenue procedure is to specify the basic requirements that the Internal Revenue Service considers to be essential in cases where a taxpayer's records are maintained within an Automatic Data Processing system (ADP). This revenue procedure updates and supersedes Rev. Proc. 91-59, 1991-2 C.B. 841.

Section 2. Background

.01 Section 6001 provides that every person liable for any tax imposed by the Code, or for the collection thereof, must keep such records, render such statements, make such returns, and comply with such rules and regulations as the Secretary may from time to time prescribe. Whenever necessary, the Secretary may require any person, by notice served upon that person or by regulations, to make such returns, render such statements, or keep such records, as the Secretary deems sufficient to show whether or not that person is liable for tax.

.02 Section 1.6001-1(a) of the Income Tax Regulations generally provides that persons subject to income tax, or required to file a return of information with respect to income, must keep such books or records, including inventories, as are sufficient to establish the amount of gross income, deductions, credits, or

other matters required to be shown by that person in any return of such tax or information.

.03 Section 1.6001-1(e) provides that the books or records required by § 6001 must be kept available at all times for inspection by authorized internal revenue officers or employees, and must be retained so long as the contents thereof may become material in the administration of any internal revenue law.

.04 Rev. Rul. 71-20, 1971-1 C.B. 392 establishes that all machine-sensible data media used for recording, consolidating, and summarizing accounting transactions and records within a taxpayer's ADP system are records within the meaning of § 6001 and § 1.6001-1, and are required to be retained so long as the contents may become material in the administration of any internal revenue law.

Section 3. SCOPE

01 Records

(1) The requirements of this revenue procedure pertain to all matters under the jurisdiction of the Commissioner of Internal Revenue including, but not limited to, income, excise, employment, and estate and gift taxes, as well as employee plans and exempt organizations.

(2) The requirements of this revenue procedure are applicable to any sections of the Code that have unique or specific record-keeping requirements. For example, machine-sensible records maintained by the taxpayer to meet the requirements of § 274(d) relating to the amount, time, place, and business purpose of a business expense must meet the requirements of this revenue procedure.

(3) Except as otherwise provided in this revenue procedure, all requirements of § 6001 that apply to hardcopy books and records apply as well to machine-sensible books and records that are maintained within an ADP system.

02 Taxpayers

(1) A taxpayer with assets of $10 million or more at the end of its taxable year must comply with the record retention requirements of Rev. Rul. 71-20 and the provisions of this revenue procedure. For purposes of this revenue procedure, a controlled group of corporations, as defined in § 1563, is considered to be one corporation, and all assets of all members of the group are aggregated.

(2) A taxpayer with assets of less than $10 million at the end of its taxable year must comply with the record retention requirements of Rev. Rul. 71-20 and

the provisions of this revenue procedure if any of the following conditions exists:

(a) All or part of the information required by § 6001 is not in the taxpayer's hardcopy books and records but is available in machine-sensible records.

(b) Machine-sensible records were used for computations that cannot be reasonably verified or recomputed without using a computer (e.g., Last-In, First-Out (LIFO) inventories).

(c) The taxpayer is notified by the District Director that machine-sensible records must be retained to meet the requirements of § 6001.

(3) A Controlled Foreign Corporation (CFC), a domestic corporation that is 25 percent foreign-owned, and a foreign corporation engaged in a trade or business within the United States at any time during a taxable year that maintains machine-sensible records within an ADP system must comply with the requirements of this revenue procedure to satisfy the record-keeping requirements of §§ 964(c), 982(d), 6038A(c)(4), and 6038C (and the regulations thereunder).

(4) An insurance company that maintains machine-sensible records within an ADP system to determine losses incurred under § 832(b)(5) must comply with the requirements of this revenue procedure and Rev. Proc. 75-56, 1975-2 C.B. 596. For this purpose, the machine-sensible records for a particular taxable year include the records for that year and the seven preceding years, all of which must be retained so long as they may become material to the examination of an insurance company's federal tax return.

(5) A taxpayer's use of a third party (such as a service bureau, time-sharing service, value-added network, or other third-party service) to provide services (e.g., custodial or management services) in respect of machine-sensible records does not relieve the taxpayer of its record-keeping obligations and responsibilities under § 6001 and this revenue procedure.

Section 4. Definitions

.01 An "ADP system" consists of an accounting or financial system (and subsystems) that processes all or part of a taxpayer's transactions, records, or data by other than manual methods. An ADP system includes, but is not limited to, a mainframe computer system, stand-alone or networked microcomputer system, Data Base Management System (DBMS), and a system that uses or incorporates Electronic Data Interchange (EDI) technology or an electronic storage system.

.02 "Capable of being processed" means the ability to retrieve, manipulate, print on paper (hardcopy), and produce output on electronic media. This term does not encompass any requirement that the program or system that created the computer data be available to process the data unless that program or system

is necessary to (1) a tax-related computation (e.g., LIFO inventories, insurance company loss reserve computations, and foreign tax credit computations); or (2) the retrieval of data (e.g., some database systems processes where the taxpayer chooses not to create a sequential extract (see section 5.02 of this revenue procedure)).

.03 A "DBMS" is a software system that creates, controls, relates, retrieves, and provides accessibility to data stored in a database.

.04 "EDI technology" is the computer-to-computer exchange of business information.

.05 An "electronic storage system" is a system used to prepare, record, transfer, index, store, preserve, retrieve, and reproduce books and records by either (1) electronically imaging hardcopy documents to an electronic storage media; or (2) transferring computerized books and records to an electronic storage media using a technique such as "COLD" (computer output to laser disk), which allows books and records to be viewed or reproduced without the use of the original program. See Rev. Proc. 97-22, 1997-13 I.R.B. 9, for electronic storage system requirements.

.06 A "machine-sensible record" is data in an electronic format that is intended for use by a computer. Machine-sensible records do not include paper records or paper records that have been converted to an electronic storage medium such as microfilm, microfiche, optical disk, or laser disk.

Section 5. Retaining Machine-Sensible Records

.01 General

(1) The taxpayer must retain machine-sensible records so long as their contents may become material to the administration of the internal revenue laws under § 1.6001-1(e). At a minimum, this materiality continues until the expiration of the period of limitation for assessment, including extensions, for each tax year. In certain situations, records should be kept for a longer period of time. For example, records that pertain to fixed assets, losses incurred under § 832(b)(5), and LIFO inventories should be kept for longer periods of time.

(2) The taxpayer's machine-sensible records must provide sufficient information to support and verify entries made on the taxpayer's return and to determine the correct tax liability. The taxpayer's machine-sensible records will meet this requirement only if they reconcile with the taxpayer's books and the taxpayer's return. A taxpayer establishes this reconciliation by demonstrating the relationship (i.e., audit trail) (a) between the total of the amounts in the taxpayer's machine-sensible records by account and the account totals in the taxpayer's books; and (b) between the total of the

amounts in the taxpayer's machine-sensible records by account and the taxpayer's return.

(3) The taxpayer must ensure that its machine-sensible records contain sufficient transaction-level detail so that the information and the source documents underlying the machine-sensible records can be identified.

(4) All machine-sensible records required to be retained by this revenue procedure must be made available to the Service upon request and must be capable of being processed.

(5) Except as otherwise required by sections 5.01(2) or (3) of this revenue procedure, a taxpayer is not required to create any machine-sensible record other than that created either in the ordinary course of its business or to establish return entries. For example, a taxpayer who does not create, in the ordinary course of its business, the electronic equivalent of a traditional paper document (such as an invoice) is not required by this revenue procedure to construct such a record, provided that the requirements of sections 5.01(2) and (3) are met. For requirements relating to hardcopy records, see section 11 of this revenue procedure.

(6) A taxpayer's disposition of a subsidiary company does not relieve the taxpayer of its responsibilities under this revenue procedure. The files and documentation retained for the Service by, or for, a disposed subsidiary must be retained as otherwise required by this revenue procedure.

.02 DBMS

(1) A taxpayer has the discretion to create files solely for the use of the Service. For example, a taxpayer that uses a DBMS may satisfy the provisions of this revenue procedure by creating and retaining a sequential file that contains the transaction-level detail from the DBMS and otherwise meets the requirements of this revenue procedure.

(2) A taxpayer that creates a file described in section 5.02(1) of this revenue procedure must document the process that created the sequential file in order to establish the relationship between the file created and the original DBMS records.

.03 EDI

(1) A taxpayer that uses EDI technology must retain machine-sensible records that alone, or in combination with any other records (e.g., underlying contracts, price lists, and price changes), contain all the information that § 6001 requires of hardcopy books and records. For example, a taxpayer that uses EDI technology receives electronic invoices from its suppliers. The taxpayer decides to retain the invoice data from completed and verified EDI transactions in its accounts payable system rather than retain the incoming EDI transactions. Neither the EDI transactions, nor the accounts payable system,

contain product descriptions or vendor names. To satisfy the requirements of § 6001, the taxpayer must supplement its EDI records with product code description lists and a vendor master file.

(2) A taxpayer may capture the required detail for an EDI transaction at any level within its accounting system. However, the taxpayer must establish audit trails between the retained records and the taxpayer's books, and between the retained records and the tax return.

(3) Section 11.02 of this revenue procedure provides additional guidance concerning hardcopy requirements related to EDI transactions.

Section 6. Documentation

.01 The taxpayer must maintain and make available to the Service upon request documentation of the business processes that (1) create the retained records; (2) modify and maintain its records; (3) satisfy the requirement of section 5.01(2) of this revenue procedure to support and verify entries made on the taxpayer's return and determine the correct tax liability; and (4) evidence the authenticity and integrity of the taxpayer's records.

.02 The documentation described in section 6.01 of this revenue procedure must be sufficiently detailed to identify

(1) The functions being performed as they relate to the flow of data through the system

(2) The internal controls used to ensure accurate and reliable processing

(3) The internal controls used to prevent the unauthorized addition, alteration, or deletion of retained records

(4) The charts of accounts and detailed account descriptions

.03 With respect to each file that is retained, the taxpayer must maintain, and make available to the Service upon request, documentation of

(1) Record formats or layouts

(2) Field definitions (including the meaning of all "codes" used to represent information)

(3) File descriptions (e.g., data set name)

(4) Evidence that periodic checks (described in section 9.01(3) of this revenue procedure) of the retained records were performed to meet section 9.02(1) of this revenue procedure, if the taxpayer wants to take advantage of section 9.02 of this revenue procedure

(5) Evidence that the retained records reconcile to the taxpayer's books

(6) Evidence that the retained records reconcile to the taxpayer's tax return.

.04 The system documentation must include any changes to the items specified in sections 6.01, 6.02, and 6.03 of this revenue procedure and the dates these changes are implemented.

Section 7. Resources

.01 The taxpayer must provide the Service at the time of an examination with the resources (e.g., appropriate hardware and software, terminal access, computer time, personnel, etc.) that the District Director determines is necessary to process the taxpayer's machine-sensible books and records. At the request of the taxpayer, the District Director may, at the District Director's discretion

(1) Identify the taxpayer's resources that are not necessary to process books and records
(2) Allow a taxpayer to convert machine-sensible records to a different medium (e.g., from mainframe files to microcomputer diskettes)
(3) Allow the taxpayer to satisfy the processing needs of the Service during off-peak hours
(4) Allow the taxpayer to provide the Service with third-party equipment

.02 An ADP system must not be subject, in whole or in part, to any agreement (such as a contract or license) that would limit or restrict the Service's access to and use of the ADP system on the taxpayer's premises (or any other place where the ADP system is maintained), including personnel, hardware, software, files, indexes, and software documentation.

Section 8. Notification

.01 Except as provided in section 9.02 of this revenue procedure, the taxpayer must promptly notify its District Director if any machine-sensible records are lost, stolen, destroyed, damaged, or otherwise no longer capable of being processed (as defined in section 4.02 of this revenue procedure), or are found to be incomplete or materially inaccurate (affected records).

.02 The taxpayer's notice must identify the affected records and include a plan that describes how, and in what timeframe, the taxpayer proposes to replace or restore the affected records in a way that assures that they will be capable of being processed. The plan must demonstrate that all of the requirements of this revenue procedure will continue to be met with respect to the affected records.

.03 The District Director will notify the taxpayer of any objections to the taxpayer's plan.

.04 A District Director may consider, whenever warranted by the facts and circumstances, the possibility of requiring less than a total restoration of missing data.

.05 Examples.

(1) Taxpayer A replaces its general ledger software system with a new general ledger software system with which the original system's records are incompatible. However, A's original records are retrievable and capable of being processed on A's hardware system. A is not required to notify its District Director of the change in its software system because A's records remain capable of being processed.

(2) Taxpayer B replaces its original ADP hardware system with a new system that cannot process the machine-sensible records created and maintained by B's original system. B must notify its District Director of this hardware system change and propose a plan for assuring that the machine-sensible records created and maintained by the original ADP hardware system are capable of being processed.

To that end, B considers the following options:

(1) Having all records in the taxpayer's original system immediately reformatted so that the new system can retrieve and process those records

(2) Having all records in its original system reformatted by a designated future date

(3) Having an arrangement with a third party to process all records in its original system on a compatible system. Any of these options may be acceptable provided the option selected enables the taxpayer to meet the requirements of this revenue procedure with respect to those records. The taxpayer must be able to demonstrate that any third-party reformatting or processing is done with the quality controls in place that will ensure the continued integrity, accuracy, and reliability of the taxpayer's records.

Section 9. Maintenance

.01 Recommended Practices

(1) The implementation of records management practices is a business decision that is solely within the discretion of the taxpayer. Recommended records management practices include the labeling of records, providing a secure storage environment, creating backup copies, selecting an offsite storage location, and testing to confirm records integrity.

(2) The National Archives and Record Administration's (NARA) Standards for the Creation, Use, Preservation, and Disposition of Electronic Records, 36

C.F.R., Ch XII, Part 1234, Subpart C (1996), is one example of a records management resource that a taxpayer may choose to consult when formulating its records management practices.

(3) The NARA standard in 36 C.F.R. § 1234.30(g)(4) (1996) requires an annual reading of a statistical sampling of magnetic computer tape reels to identify any loss of data and to discover and correct the causes of data loss. In libraries with 1,800 or fewer storage units (e.g., magnetic tape reels), a 20 percent random sampling or a sample size of 50 units, whichever is larger, should be read. In libraries with more than 1,800 units, a sample of 384 units should be read. Although this NARA sampling standard is specifically for magnetic computer tape, the Service recommends that all retained machine-sensible records be sampled and tested as described in the NARA standard.

.02 Partial Loss of Data

A taxpayer that loses only a portion of the data from a particular storage unit will not be subject to the penalties described in section 12 of this revenue procedure if the taxpayer can demonstrate to the satisfaction of the District Director that the taxpayer's data maintenance practices conform with 36 C.F.R. § 1234.30(g)(4) (1996) (the NARA sampling standard). However, the taxpayer remains responsible for substantiating the information on its return as required by § 6001.

Section 10. District Director Authority

.01 Record Retention Limitation Agreement

(1) A taxpayer who maintains machine-sensible records may request to enter into a Record Retention Limitation Agreement (RRLA) with its District Director. This agreement provides for the establishment and maintenance of records as agreed upon by the District Director and the taxpayer.

(2) The taxpayer's request must identify and describe those records the taxpayer proposes not to retain and explain why those records will not become material to the administration of any internal revenue law. The District Director will notify the taxpayer whether or not the District Director will enter into an RRLA.

(3) In an RRLA, the District Director may waive all or any of the specific requirements in this revenue procedure. A taxpayer remains subject to all the requirements in this revenue procedure that are not specifically modified or waived by an RRLA.

(4) Unless an RRLA otherwise specifies, an RRLA shall not apply to accounting and tax systems added subsequent to the completion of the record evaluation upon which the agreement is based. All machine-sensible records produced by a subsequently added accounting and tax system, the contents of which may be or may become material in the administration of the Code, must be

retained by the taxpayer signing the RRLA until a new evaluation is conducted by the District Director.

(5) Unless an RRLA specifies otherwise, it does not apply to a subsidiary acquired subsequent to the completion of the record evaluation upon which the RRLA is based. All machine-sensible records produced by the acquired subsidiary, the contents of which may be or may become material in the administration of the Code, must be retained pursuant to this revenue procedure and any pre-acquisition RRLA ("former RRLA") that applies to the acquired subsidiary. The former RRLA applies to the acquired subsidiary until the District Director either revokes the former RRLA (in whole or in part) or enters into a new RRLA that applies to the acquired subsidiary.

(6) Upon the disposition of a subsidiary, the files being retained for the Service pursuant to an RRLA by, or for, the disposed subsidiary must be retained by the taxpayer until a new evaluation is conducted by the District Director.

(7) A District Director's decision to revoke an RRLA, or not to enter into an RRLA, does not relieve the taxpayer of its recordkeeping obligations under § 6001 or its responsibilities described in this revenue procedure.

.02 Records Evaluation

(1) The District Director may conduct a records evaluation at any time the District Director deems it appropriate to review the taxpayer's record retention practices, including the taxpayer's relevant data processing and accounting systems.

(2) The records evaluation described in section 10.02 (1) of this revenue procedure is not an "examination," "investigation," or "inspection" of the books and records within the meaning of § 7605 (b) of the Code, or a prior audit for purposes of § 530 of the Revenue Act of 1978, 1978-3 (Vol. 1) C.B. 119, as amended by § 1122 of the Small Business Job Protection Act of 1996, because this evaluation is not directly related to the determination of the tax liability of a taxpayer for a particular taxable period.

(3) The District Director will inform the taxpayer of the results of a records evaluation.

.03 Testing

(1) The District Director may periodically initiate tests to establish the authenticity, readability, completeness, and integrity of a taxpayer's machine-sensible records retained in conformity with this revenue procedure.

(2) These tests may include a review of integrated systems such as EDI or an electronic storage system, and a review of the internal controls and security procedures associated with the creation and maintenance of the taxpayer's records.

(3) The tests described in section 10.03(1) of this revenue procedure are not an "examination," "investigation," or "inspection" of the books and records

within the meaning of § 7605(b) of the Code, or a prior audit for purposes of § 530 of the Revenue Act of 1978, 1978-3 (Vol. 1) C.B. 119, as amended by § 1122 of the Small Business Job Protection Act of 1996, because these tests are not directly related to the determination of the tax liability of a taxpayer for a particular taxable period.

(4) The District Director will inform the taxpayer of the results of these tests.

Section 11. Hardcopy Records

.01 The provisions of this revenue procedure do not relieve taxpayers of their responsibility to retain hardcopy records that are created or received in the ordinary course of business as required by existing law and regulations. Hardcopy records may be retained in microfiche or microfilm format in conformity with Rev. Proc. 81-46, 1981-2 C.B. 621. Hardcopy records may also be retained in an electronic storage system in conformity with Rev. Proc. 97-22. These records are not a substitute for the machine-sensible records required to be retained by this revenue procedure.

.02 A taxpayer need not create or retain hardcopy records if

(1) The hardcopy records are merely computer printouts created only for validation, control, or other temporary purposes

(2) The hardcopy records are not produced in the ordinary course of transacting business (as may be the case when utilizing EDI technology)

(3) All the details relating to the transaction are subsequently received by the taxpayer in an EDI transaction and are retained as machine-sensible records by the taxpayer in conformity with this revenue procedure. For example, a taxpayer need not retain credit card receipts generated at the time of a transaction if all pertinent information on the receipts is subsequently received in an EDI transaction and retained as a machine-sensible record. See section 5.03 of this revenue procedure for requirements relating to EDI.

.03 A taxpayer need not create hardcopy printouts of its machine-sensible records unless requested to do so by the Service. The Service may request such hardcopy printouts either at the time of an examination or in conjunction with the tests described in Section 10.03(1) of this revenue procedure.

APPENDIX C: FINANCIAL INSTITUTION RULES FROM GLB

II. Standards for Safeguarding Customer Information

A. Information Security Program. Each bank shall implement a comprehensive written information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the bank and the nature and scope of its activities. While all parts of the bank are not required to implement a uniform set of policies, all elements of the information security program must be coordinated.

B. Objectives. A bank's information security program shall be designed to
   1. Ensure the security and confidentiality of customer information
   2. Protect against any anticipated threats or hazards to the security or integrity of such information
   3. Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer

III. Development and Implementation of Information Security Program

A. Involve the Board of Directors. The board of directors or an appropriate committee of the board of each bank shall
   1. Approve the bank's written information security program
   2. Oversee the development, implementation, and maintenance of the bank's information security program, including assigning specific responsibility for its implementation and reviewing reports from management.

B. Assess Risk. Each bank shall
   1. Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems.
   2. Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information.
   3. Assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks.

C. Manage and Control Risk. Each bank shall
   1. Design its information security program to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of the bank's activities. Each bank must consider whether the following security measures are appropriate for the bank and, if so, adopt those measures the bank concludes are appropriate:

a. Access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals, and controls to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means
b. Access restrictions at physical locations containing customer information, such as buildings, computer facilities, and records storage facilities, to permit access only to authorized individuals
c. Encryption of electronic customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access
d. Procedures designed to ensure that customer information system modifications are consistent with the bank's information security program
e. Dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to customer information
f. Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems
g. Response programs that specify actions to be taken when the bank suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies
h. Measures to protect against destruction, loss, or damage of customer information due to potential environmental hazards, such as fire and water damage or technological failures.

2. Train staff to implement the bank's information security program.
3. Regularly test the key controls, systems, and procedures of the information security program. The frequency and nature of such tests should be determined by the bank's risk assessment. Tests should be conducted or reviewed by independent third parties or staff independent of those that develop or maintain the security programs.

D. Oversee Service Provider Arrangements. Each bank shall
1. Exercise appropriate due diligence in selecting its service providers
2. Require its service providers by contract to implement appropriate measures designed to meet the objectives of these Guidelines
3. Where indicated by the bank's risk assessment, monitor its service providers to confirm that they have satisfied their obligations as required by paragraph D.2. As part of this monitoring, a bank should review audits, summaries of test results, or other equivalent evaluations of its service providers

E. Adjust the Program. Each bank shall monitor, evaluate, and adjust, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its customer information, internal or external threats to information, and the bank's own changing business arrangements,

such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to customer information systems.

F. Report to the Board. Each bank shall report to its board or an appropriate committee of the board at least annually. This report should describe the overall status of the information security program and the bank's compliance with these Guidelines. The report, which will vary depending upon the complexity of each bank's program, should discuss material matters related to its program, addressing issues such as risk assessment; risk management and control decisions; service provider arrangements; results of testing; security breaches or violations, and management's responses; and recommendations for changes in the information security program.

In the event of pandemic influenza, businesses will play a key role in protecting employees' health and safety as well as limiting the negative impact to the economy and society. Planning for pandemic influenza is critical. To assist you in your efforts, the Department of Health and Human Services (HHS) and the Centers for Disease Control and Prevention (CDC) have developed the following checklist for large businesses. It identifies important, specific activities large businesses can do now to prepare, many of which will also help you in other emergencies. Further information can be found at http://www.pandemicflu.gov and http://www.cdc.gov/business.

APPENDIX D: Checklist for Pandemic Planning

Plan for the impact of a pandemic on your business

Tasks	Not Started	In Progress	Completed
Identify a pandemic coordinator or team with defined roles and responsibilities for preparedness and response planning. The planning process should include input from labor representatives.			
Identify essential employees and other critical inputs (e.g., raw materials, suppliers, subcontractor services/ products, and logistics) required to maintain business operations by location and function during a pandemic.			
Train and prepare ancillary workforce (e.g., contractors, employees in other job titles/ descriptions, retirees).			
Develop and plan for scenarios likely to result in an increase or decrease in demand for your products or services during a pandemic (e.g., effect of restriction on mass gatherings, need for hygiene supplies).			
Determine potential impact of a pandemic on company business financials using multiple possible scenarios that affect different product lines or production sites.			
Determine potential impact of a pandemic on business-related domestic and international travel (e.g., quarantines, border closures).			
Find up-to-date, reliable pandemic information from community public health, emergency management, and other sources, and make sustainable links.			
Establish an emergency communications plan and revise periodically. This plan includes identification of key contacts (with backups), chain of communications (including suppliers and customers), and processes for tracking and communicating business and employee status.			
Implement an exercise/drill to test your plan, and revise periodically.			

Plan for the impact of a pandemic on your employees and customers

Tasks	Not Started	In Progress	Completed
Forecast and allow for employee absences during a pandemic due to factors such as personal illness, family member illness, community containment measures and quarantines, school or business closures, and public transportation closures.			
Implement guidelines to modify the frequency and type of face-to-face contact (e.g., handshaking, seating in meetings, office layout, shared workstations) among employees and between employees and customers (refer to CDC recommendations).			
Encourage and track annual influenza vaccination for employees. .			
Evaluate employee access to and availability of healthcare services during a pandemic, and improve services as needed.			
Evaluate employee access to and availability of mental health and social services during a pandemic, including corporate, community, and faith-based resources, and improve services as needed. .			
Identify employees and key customers with special needs, and incorporate the requirements of such persons into your preparedness plan.			

Establish policies to be implemented during a pandemic

Tasks	Not Started	In Progress	Completed
Establish policies for employee compensation and sick-leave absences unique to a pandemic (e.g., nonpunitive, liberal leave), including policies on when a previously ill person is no longer infectious and can return to work after illness.			
Establish policies for flexible worksite (e.g., telecommuting) and flexible work hours (e.g., staggered shifts).			
Establish policies for preventing influenza spread at the worksite (e.g., promoting respiratory hygiene/ cough etiquette, and prompt exclusion of people with influenza symptoms).			
Establish policies for employees who have been exposed to pandemic influenza, are suspected to be ill, or become ill at the worksite (e.g., infection control response, immediate mandatory sick leave).			
Establish policies for restricting travel to affected geographic areas (consider both domestic and international sites), evacuating employees working in or near an affected area when an outbreak begins, and guidance for employees returning from affected areas (refer to CDC travel recommendations).			
Set up authorities, triggers, and procedures for activating and terminating the company's response plan, altering business operations (e.g., shutting down operations in affected areas), and transferring business knowledge to key employees.			

Allocate resources to protect your employees and customers during a pandemic

Tasks	Not Started	In Progress	Completed
Provide sufficient and accessible infection control supplies (e.g., hand-hygiene products, tissues and receptacles for their disposal) in all business locations.			
Enhance communications and information technology infrastructures as needed to support employee telecommuting and remote customer access.			
Ensure availability of medical consultation and advice for emergency response.			

Communicate to and educate your employees

Tasks	Not Started	In Progress	Completed
Develop and disseminate programs and materials covering pandemic fundamentals (e.g., signs and symptoms of influenza, modes of transmission), personal and family protection and response strategies (e.g., hand hygiene, coughing/ sneezing etiquette, contingency plans).			
Anticipate employee fear and anxiety, rumors and misinformation, and plan communications accordingly.			
Ensure that communications are culturally and linguistically appropriate.			
Disseminate information to employees about your pandemic preparedness and response plan.			
Provide information for the at-home care of ill employees and family members.			
Develop platforms (e.g., hotlines, dedicated Web sites) for communicating pandemic status and actions to employees, vendors, suppliers, and customers inside and outside the worksite in a consistent and timely way, including redundancies in the emergency contact system.			
Identify community sources for timely and accurate pandemic information (domestic and international) and resources for obtaining countermeasures (e.g., vaccines and antivirals).			

Coordinate with external organizations and help your community

Tasks	Not Started	In Progress	Completed
Collaborate with insurers, health plans, and major local healthcare facilities to share your pandemic plans and understand their capabilities and plans.			
Collaborate with federal, state, and local public health agencies or emergency responders to participate in their planning processes, share your pandemic plans, and understand their capabilities and plans.			
Communicate with local or state public health agencies or emergency responders about the assets or services your business could contribute to the community.			
Share best practices with other businesses in your communities, chambers of commerce, and associations to improve community response efforts.			

Handling of Sensitive Information (Example HIPAA Compliance)

Application of HIPAA Class Security to Disaster Recovery

Most people think of disaster recovery only as the planned response to a formally declared disaster. To fall into this trap is to ignore the safeguarding of data at all other times. Failure to safeguard data at all other times may result in a declared disaster. How many times in recent months have you heard on the news that an institutions' security has been compromised, and that up to 250,000 credit card accounts have been stolen at one time? When you stop for a moment and consider that many pieces of personal information are related to each credit card account, you come to the unmistakable conclusion that up to 250,000 people believe that a disaster has just occurred because their personal data has been stolen.

Absolute data security is a myth. There is a mathematical statement that establishes the number of rules required to define any situation as Nr = rules + 1. The reality of this statement is that no matter how many rules you conceive or write, one more is always required to complete the specification. In other words, you can never write enough rules to completely cover any given situation. As demonstrated by two

Israeli graduate students, what was considered by the National Security Agency (NSA) just a short few years ago to be an unbreakable security scheme could be broken by concerted and dedicated efforts in a relatively short time with simple PCs. This author believes that a layered approach to security is the best possible defense against any form of security threat.

The U.S. Congress enacted the Health Insurance Portability and Accountability Act of 1996 (HIPAA), on Aug 21, 1996. The U.S. Department of Health and Human Services (HHS) was required by the Act to issue privacy regulations if Congress did not enact privacy legislation within three years. A set of rules proposed by HHS was posted for public comment in November 1999, and after 52,000 public comments were considered, the rule was published on December 28, 2000. On August 14, 2002, modifications to the rules were published after consideration of 11,000 public comments.

The rules established by HHS as a result of this piece of legislation directly affect all who come into contact with health data, whether patient, health services provider, or anyone else such as a contractor or computer programmer. This data is very personal in nature. It is impossible in today's world to obtain health services without providing additional personal data such as social security number, address, contact phone numbers, next-of-kin information, and birth date to health service providers. Clearly, there is enough personal information floating around in the commercial world (financial institutions of all kinds and those businesses that depend upon financial services such as home sales or auto sales) to make identity theft a very real concern to individuals and businesses.

To protect against the threat of potential disaster, many, if not most, large and medium sized businesses have completed the task of creating and implementing a disaster recovery plan. These plans nearly always call for the storage of critical company data in a secure offsite storage facility. In today's world, the necessity of frequently moving critical data to off-site storage involves either dedicated point-to-point high-speed electronic transmission facilities or the use of the public Internet. Even dedicated point-to-point high-speed electronic transmission facilities can be viewed or captured by unscrupulous service personnel or communications providers. The public Internet traverses so many different providers that the possibility of data being viewed or captured by unscrupulous service personnel is greatly magnified.

Whether data is electronically transmitted to an off-site storage facility for disaster recovery purposes or is hand carried to that facility via magnetic tape, DVD, CD-ROM, or other storage media, there is a need to protect the data. A layered approach to security will provide the best possible deterrent to those bent on obtaining access to private business and personal data. This author believes that the layered approach to data security must be implemented in addition to traditional physical data security.

The layered approach to security can be likened to the layers one finds in an onion; there the data has been hidden deep inside at the center. To get at the data inside, the thief finds another layer beneath the one he has just breached. Each successive layer

should be constructed to be more resilient than the preceding one. Hopefully, the thief will encounter a layer that he cannot breach, or so much time will be consumed in his efforts to crack the layer that he will be caught before doing so.

If data is being transmitted electronically via the public Internet, then all possible security layers should be used. When nonpublic electronic transmissions are being used, one should use as many security layers as possible.

What security layers are possible? Let us look at some real-world situations. Let us start with a worst-case scenario. As a test case, let us choose daily electronic transmissions of sensitive data over the public Internet as many small, medium, and even large businesses do.

Before we continue with our test case, consider that it would not be appropriate to attach an unencrypted data file to an e-mail and send it to a secure off-site storage facility. This mechanism is mentioned only to draw attention to the sending of data in blocks or large chunks commonly known as data files. Because of size and efficiency limitations inherent in e-mail systems, a different form of managing data transmissions is called for. File Transfer Protocol, or FTP, has been around for many years. Its evolution has been progressive, and FTP systems now contain many desirable features. They are available on computers small and large, from PCs to mainframes.

An FTP system consists of two software components — a host and a remote client. The host is traditionally viewed as being local, and the client is viewed as being remote (from the host, that is) as long as it resides on a different computer. An FTP system is normally designed to allow the host component to provide overall control, being able to accept or reject any or all transmission attempts from any given FTP client. The FTP client component generally initiates the transmission attempt to the host and, after a successful session is established, begins transferring data only as allowed by the host.

An FTP session can be viewed as consisting of three separate but related processes. First, there is session establishment or "logon," which includes negotiation over identification (user ID) and password. Second, there is session control, and third, there is data transfer. These three processes can be viewed as three separate but related channels, all of which are necessary to accomplish the transfer of data between two computers. These related channels are the identification channel, command and control channel, and the data channel. If each of these channels is made secure, each using a different security mechanism, then we will have achieved a layered approach to the security of file transfers.

The preceding ideas are not new, nor are they unique. Indeed, they have been around long enough to be incorporated into various products with varying degrees of success. It is not this author's intent to provide a review of or to recommend any particular product. The preceding discussion and that which is to follow is intended to tickle and stimulate your imagination. Merely knowing that a layered approach in secure electronic data transmission is possible will allow you to ferret out tools that will meet your individual or specific needs.

To make session establishment or the logon channel as secure as possible, the negotiation of user ID and password must be completed using encrypted values. Not all FTP systems support this very important first step. It is also necessary that all access to the FTP host be strictly limited to only the FTP clients required to complete the data transfers. All access to the FTP host by FTP clients other than those required must be prevented; otherwise, the potential for disaster increases. Anonymous access to the FTP host should never be allowed. Once again, not all FTP systems support these constraints, but some do. A simple product search will find those that are capable.

Even though encrypted, the user ID and password should not be trivial values. Shorter values (user ID and password) are easier to crack or decode. Did you know that because of the way some operating systems software implement password encryption, a thirteen- or fourteen-character password is the most difficult to crack? In other words, in some systems, fewer than or more than thirteen or fourteen characters yield a less secure password. A trivial password value is a value that can be easily guessed because of its association with a particular function or with specific personnel. Ideally, a random and long string of letters and numbers is best. A random mix of upper and lower case letters along with numbers should always be used in the password. Values such as people's names, birth dates, and names of children or pets are always trivial because an industrious hacker can easily determine them.

Once the logon channel negotiation is complete, it is best if a different security mechanism is implemented in the command and control channel. The industry has evolved a fairly secure mechanism known as "secure sockets layer" that can be and indeed has been implemented in the command and control channel of some available FTP products. A Web search will result in a vast amount of information on "secure sockets layer." A tutorial on "secure sockets layer" is not the purpose of this book because much material is already available. By the by, a typical "secure sockets layer" is currently typically based upon a 128-bit key. However, it is recommended that the highest possible key length be used at all times. A 156-bit key length is rapidly gaining wide implementation with even larger keys available in some products. Even larger key lengths will follow in the future.

The "secure sockets layer" security mechanism encrypts the commands and controls flowing in the command and control channel. This channel allows the FTP client to put the data files into the allowed locations on the FTP host computer. It is recommended that each authorized FTP client be completely constrained to uploading data files only into one set of directories or destination paths. If this is done, then a hacker will not be able to roam freely through the computer even if security is breached at this level. Some FTP systems even require that all configuration changes be made under unique user ID and password control.

It is possible to improve upon the security used within the command and control channel. Using Secure Shell (SSH) achieves this. SSH provides improved security because it invokes Secure File Transfer Protocol (SFTP). This combination of

SSH and SFTP results in the encryption of all information in the command and control channel and in the data channel.

The final channel to be considered is the data channel. After a secure logon is achieved, and secure command and control is in place, the data can finally be transferred. If we encrypt the data before transmission, then we will have achieved our strived-for layered approach to secure electronic transmission of data using the public Internet. If an industrial-strength encryption mechanism such as OpenPGP is used, then we will have used a completely different security mechanism in each of the three FTP channels.

OpenPGP is an open implementation of Pretty Good Privacy that can be found by doing a Web search. Some FTP systems that are currently available have this security tool built in to be used within its data channel. Open PGP is a two-key security mechanism that encrypts the data using a public key and then uses a private decryption key that only the intended recipient has a copy of. The key, if you will, is to ensure that no one else ever obtains a copy of the private key. Steps must be taken to protect the private key at all costs. The converse is also true. Disaster recovery planning steps must be taken to ensure that the data owner always has a copy of the private key, or else even the data owner may never be able to decrypt his own data. Building these steps into your disaster recovery plan is of utmost importance but is not necessarily easy.

The key to the strength of OpenPGP is the use of very long keys that are inherently hard to crack. A typical key length is 2048 to 4096 bits. Longer keys are possible, but really long keys may result in performance issues on some computers. As discussed previously, the longest key consistent with hardware performance limitations is always recommended.

The final and last item to consider is that of ensuring that adequate logging of all steps of the file transfer process takes place and that an adequate means of analyzing the logs is in place. Analysis of the logs must be able to reveal whether the data transfers take place as intended and whether there are any outside intrusion attempts being made.

As you can readily see from the preceding discussion, our concern here is the protection of data during transit. If data is being transferred electronically whether over point-to-point facilities or over a public network such as the Internet, then it is recommended that an FTP system having all channels protected by a different secure mechanism is not just recommended but should be considered to be a requirement. For those businesses that are relying upon physical transfer of storage media, it is recommended that the data be encrypted using a highly secure mechanism such as OpenPGP before being committed to the storage media used in transfer.

It must be emphasized that no amount of caution and rule writing can guarantee absolute security of data. The best that we can do is to make theft so difficult that the thief gives up before achieving success.

Lessons to be learned from this: (1) Congress needs to have a tutorial covering the basic mathematics behind rule making (laws). Seriously, just because it is not possible to ever get there rulewise, is no reason not to be as diligent as possible, and layering multiple security mechanisms seems like a good way to go. (2) Take heart, it's not as difficult as it might seem because others have already been there and done that.

Good luck! Make it as tough as you can on the thieves of the world, but remember what you learned about rule making and layering.

Chapter 10

Sarbanes–Oxley Act of 2002

David P. Mowery

Contents

Introduction 337
A New Direction 340
Reporting..... 344
Impact on Smaller Firms..... 346
Impact of SOX on the Board of Directors.....347
Whistle-Blowers.....349
Review of Other Highlights of the Act 349

Introduction

Why There Was a Need

By now we have all heard the story of the whistle-blower at Enron who called the Securities and Exchange Commission (SEC) to report the questionable accounting practices at Enron. She was brought before an attorney to tell her story. Nothing happened for a year, so after that time she called back to see if they were going to investigate. By then her conscience and morals were starting to cause problems for her.

This time, however, when turned over to another attorney to explain her problems, she asked, "Don't you have any CPAs there that I can talk to?" In response, she was referred to an accountant instead of an attorney. He not only understood but also was amazed at her story and launched an investigation. The rest, as they say, is history.

- WorldCom tells a different story with the same ending. It weaves a tale of excessive loans to corporate officers to buy lavish homes and golf courses. Millions of dollars in expenses were hidden through capitalization and write-offs over a period of seven years.
- This same type of structuring was tried by Dollar General. That firm's CFO did not post an accrual of several million dollars in freight costs from overseas. He later convinced the auditors to just write off the expenses over the next 12 months, rather than restate the 1999 figures. For his actions, the CFO finally agreed to a $1,300,000 fine by the SEC.
- Ben & Jerry's CFO is off to jail for 27 months for embezzling nearly $300,000 from his employer.
- The story of Qwest was one of highly inflated sales to generate sales commissions. Sales were overstated by $10,000,000. This one at least did not end in bankruptcy, but still reflects a growing lack of ethics in big business. Executives lost their jobs, and investors lost value in their investments. But Qwest was not the only one to pad Sales and Accounts Receivable, and it was by no means the company with the largest overstatement.

The list grows daily. A growing lack of loyalty to the company they work for, the board they serve on, the stockholders they are supposed to protect, and the employees who work for them seems to be running rampant throughout big business. It would take a two-day seminar to just cover the companies that have been caught in the United States. Europe is not exempt. The same thing happened there. It started with the external auditors not following auditing standards that every first-year graduate should know.

The Creation of the Law

To sum it up, Congress had had enough. They went to the SEC and complained of lack of oversight. The SEC was technically in charge but had done nothing about the problems. They had left it up to the AICPA (American Institute of Certified Public Accountants) and the Institute of Management Accountants (IMA), instead. These accounting associations failed the American public as de facto oversight bodies.

The SEC was ordered to take charge and prepare a fix for this problem, or an office would be founded that could and would fix the problem. Granted, this is an oversimplification of what happened, but it covers the results.

At this point, the SEC began work on its investigation and the draft of a new law. It was almost as if, in the course of the investigation, every time an irregularity was seen or a mistake was observed, a note was made of the infraction. Then all the notes were assembled in a draft of a new law that would hopefully cure the problem. This new law would do the following:

- Tell management what they must do
- Tell the internal auditors what they must do
- Tell the external auditors what they must do

Then, to ensure compliance, stiff penalties (real and personal) were added, which included jail time and personal fines.

The draft of the new law, which included the formation of a new board — the Public Company Accounting Oversight Board (PCAOB) — was forwarded to Congress where Paul Sarbanes and Mike Oxley championed it. The Sarbanes–Oxley Act was enacted in July, 2002. It begins as follows:

> To protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities law.

The PCAOB reports directly to the SEC, who in turn enforces the decisions of the PCAOB and levies the fines. The PCAOB is made up of five accounting-literate members. Two of the members must be or should have been CPAs and the other three members cannot be and should never have been CPAs. The chairman of the board may be one of the CPAs but, if so, he or she should not have been a practicing CPA for the last five years.

The PCAOB regulates the audits and ethical standards of publicly traded companies. They are charged with promulgating auditing and related attestation and ethics standards for audits and reviews of these companies.

To audit a public company, the CPA firm must register with the PCAOB and are subject to audit and inspection by the PCAOB. If the CPA firm audits 100 or more publicly traded companies, they must be audited every year. If the CPA firm audits less, they must be audited every three years.

After the first year, the PCAOB audited the "Big 4." All failed the inspection. The PCAOB refused to give out the grades or reports as it could upset the small balance and independence that was left after the death of the Arthur Anderson CPA firm and consolidation of the others. They are now reporting the results of their audits on the Web site http://www.pcaobus.org/Inspections/Public_Reports/index.aspx.

Nothing New

The concentration on a corporation's internal control is anything but new. Beginning in the early 1980s, the Gaming Control Board in Nevada required that all casinos flowchart their gaming proceedings as well as obtain approval by the board. Later, the external auditor's annual audit had to include an audit of the casino's compliance with its own procedures. A separate audit report had to be sent to the board with a notation of every time the casino violated its own procedures.

The external auditors normally drew up the control procedure and then audited compliance.

Each internal control procedure in a corporation must be charted. The external auditor cannot prepare the report, help prepare the report, or even make suggestions. If they find something wrong with the report, they must not tell exactly what is wrong. There must be total independence of the external auditor.

In the past, the SEC, because of stock ownership in companies that they were auditing, threatened many Big 8 partners, managers, and supervisors with sanctions. With SOX, I am sure this will be addressed again.

A New Direction

Management Responsibilities

With the advent of SOX, the management's responsibility for internal control, operations, and the financial statements are reinforced. A new emphasis is placed on organizational responsibilities and corporate governance.

Management must now provide personal assurance with regard to internal control. It is no longer acceptable to dismiss operations with the phrase, "to the best of my knowledge." CEOs and CFOs must now assert that the operations and internal control are tight enough to prevent fraud — both misappropriation and misrepresentation. This must be realized through the section 404 procedures, discussed at the end of this chapter. It is through analysis of the internal control procedures dictated in section 404 that the CEO and CFO will be able to make an assessment of internal control.

Unfortunately for management, this assessment must be positive, or they are required to report all areas of weakness to the auditors through the audit committee. It then becomes the responsibility of the auditors to review the same procedure manuals that management used to make their decisions and attest to the assurance of management.

Unlike procedures in the past, the auditors may not assist in the development or documentation of these procedures. After review, the auditors may not make recommendations to management on how to improve these procedures. Management must then respond to the auditor's negative comments on internal control procedures.

This is not a one-time or even annual procedure. The requirement is for the assurance to be submitted with the annual audit filing as well as all quarterly filings to the SEC. All failures of internal control must be reported with all filings.

To ensure compliance with these guidelines, the SOX Act has established significant penalties in Section 1350: "Failure of corporate officers to certify financial reports." Whoever does not comply with the certification of financial reports

as outlined in paragraphs a and b of this section "shall be fined not more than $1,000,000.00 or imprisoned not more than 10 years, or both."

Furthermore, whoever willfully certifies to the correctness of the internal control and certifies that the reports present fairly the financial condition and the results of operation knowing that they do not comport with all the requirements, "shall be fined not more than $5,000,000.00, or imprisoned more than 20 years, or both."

These are not company fines and penalties but personal fines and penalties.

Ethics

Section 406 of the law — Code of Ethics for Senior Financial Officers.

However, we have to ask ourselves the all-important question, "At our age, can ethics be taught?" I think not. For the ethical, it's reinforcement. For those struggling with the decision, it's help to make the right decision. For the unethical, the most one can hope for is that it instills the fear in them to do what is right. They can't afford the fines, they fear prison, and, mostly, they fear the shame and embarrassment of being caught. Something that scares the unethical enough should make them at least think about it before committing fraud.

SOX did set up new or, at least, reinforced old standards:

- It is a reminder that accounting firms must be independent.
- The audit partner must rotate off the audit every five years.
- The auditors will be chosen by, and report directly to, the audit committee of the board of directors. (And, yes, every board must have an audit committee!)
- To avoid conflicts of interest, the CEO, CFO, and Chief Accounting Officer, or their equivalents should not have been employed by a company's audit firm during the prior year.
- Audit companies must be inspected by the PCAOB annually if they audit 100 or more publicly traded companies. If less, they must be inspected at least every three years.

In keeping with the theme of ethics throughout the law, CPAs are reminded that they have a special duty to society and must follow the spirit of the law rather than search out loopholes. In addition, the company is expected to establish, in writing, a code of professional ethics. This code is for senior financial officers and deals with handling outside business interests. It should include guidelines on fiduciary relationships and the purchase of corporate assets. Besides reviewing dealings with outside directorships, partnerships and personal companies, it should also deal with nonbusiness activities.

The company needs to deal with illegal and unethical acts, gifts, fees, borrowing for the company and related parties, as well as misappropriation of business opportunities. Regardless of manuals and codes of ethics, it comes down to our initial discussion of ethics. Ethical business practices will be controlled by strong internal control procedures.

Two things that must be remembered:

1. Internal control is only as good as the management enforcing it.
2. The person taking advantage of weaknesses in internal control will never be a person you don't trust. The person you *don't* trust will never get the opportunity. It shall always be the person you *do* trust, because that's the person you will not be watching.

SAS 99 and PCAOB Auditing Standards

In October 2002, the AICPA's Auditing Standards Board issued SAS 99, Consideration of Fraud in a Financial Statement Audit.

The PCAOB has stated that they expect auditors to consider this statement in the audit of a public company. The key factors of this statement include the fraud triangle, which is usually present whenever fraud occurs (see Figure 10.1). It consists of:

1. Pressure
2. Opportunity
3. Rationalization

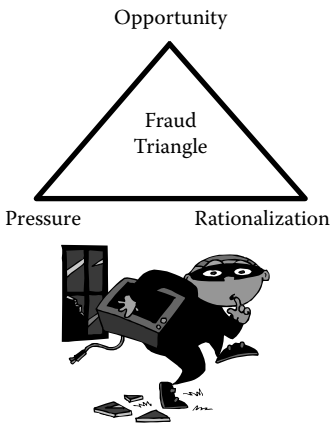


Figure 10.1 The fraud triangle.

Pressure

An ethical, trusted employee commits most fraud. He or she gets in a bind. It might be a sick wife or child, a spendthrift in the family, an emergency, or keeping up with the neighbors. Whatever it is, it is usually something that he or she is too uncomfortable with, or embarrassed by, to discuss with his fellow employees or boss.

Usually it is a "one-time occurrence" that the employee fully intends to pay back. At least, in the beginning.

Opportunity

The second factor in the triangle is the opportunity. Again, as I stated earlier, it is the trusted employees who find an opportunity to commit fraud for any length of time. The ones you don't trust are the ones you are always watching. They may get away with fraud for a short time, but they will be caught.

Although the employees may have intended to pay it back, they never get caught up enough to have extra money. Unfortunately, each time they "borrow" from their company, it gets easier.

Rationalization

Soon, it becomes impossible to pay back. The employee is too far in debt. But, so what if he or she takes this money? If the company were paying the employee what he or she was worth, the employee wouldn't have to take money. Besides, every one else is doing it. And it's built into the cost of sales. The company probably has insurance, so it's no big deal. Now we're no longer a thief. We're doing what the company "expects," and "budgets" for us to do.

This is the typical pattern; however, some employees do indeed go to work with the original intent to commit fraud. This can happen when the supervisor is a very trusting individual and hires the "perfect applicant." The supervisor never considers that the new employee might be a thief. They came with such good recommendations. For these persons, the opportunity is all that is needed. They *will* be caught; it is just a matter of how much they will get away with before they are caught.

Regardless of the explanation of the points of the triangle, the bottom line is that the auditor must be looking for fraud when he or she audits, as this could result in a material misstatement of the financial statements.

With SAS 99, the following become important steps in the audit:

- Discuss the risk of material misstatement of the financial statements because of fraud.
- Discuss where the statements might most likely be materially misstated because of fraud.
- Identify the risk areas.
- Assess the risk and risk areas.
- Discuss and evaluate areas that are discovered in the course of the audit.

PCAOB carried it even further. To date, the PCAOB has finalized three auditing standards and proposed a fourth.

The first statement, References in Auditors' Reports to the Standards of the Public Company Accounting Oversight Board, directs auditors of publicly traded companies to state that the audit was conducted in accordance with "the standards of the Public Company Accounting Oversight Board (United States)." Although it

was very short, it said a lot. The AICPA no longer sets the audit standards for auditing publicly traded companies.

The second statement, An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements, addresses how to audit management's assessment of the internal control. This is the same assessment that management has certified as to "the effectiveness of the internal control structure and procedures of the issuer for financial reporting." (Section 404, SOX) The PCAOB has identified 13 key provisions in this standard. Section 404 is very short but has cost Fortune 500 corporations millions to comply with. This section alone has been the subject of week-long seminars.

Statement #3, Audit Documentation, covers the documents that auditors need to generate and retain in an audit or review. Any change to the work papers after the engagement must be done within 45 days. The papers must be retained for seven years.

Reporting

The Standards as Outlined in the "Letter"

Auditing standards have always required that the letter attached to each audited financial statement reference the standards established by the AICPA and the auditor state that the financial statements conform to Generally Accepted Accounting Principles (GAAP).

The new regulations require the letter to reference the standards established by PCAOB for all statements issued or reissued after May 24, 2004. The following is an example of this letter on an audit of financial statements:

> We have audited the accompanying Balance Sheet of X Company as of December 31, 20XX, and the related statements of operations, shareholders' equity, and cash flows for each of the three years in the period ended December 31, 20XX. These financial statements are the responsibility of the Company's management. Our responsibility is to express an opinion on these financial statements based on our audits.
>
> We conducted our audits in accordance with the standards of the Public Company Accounting Oversight Board (United States). Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement.
>
> An audit includes examining, on a test basis, evidence supporting the amounts and disclosures in the financial statements. An audit also includes assessing the accounting principles used and significant

> estimates made by the management, as well as evaluating the overall financial statement presentation. We believe that our audits provide a reasonable basis for our opinion.
>
> In our opinion, the financial statements referred to above present fairly, in all material respects, the financial position of the company as of December 31, 20XX and 20XX (with the most recent year first), and the results of its operation and its cash flows for each of the three years in the period ended December 31, 20XX, in conformity with U.S. Generally Accepted Accounting Principles.

With this letter, the AICPA no longer has the final say on financial statement presentation for publicly traded companies.

Internal Control

The changes in internal control are vital to the success of the Sarbanes–Oxley Bill. The internal auditor no longer reports to management but to the audit committee. It is up to the audit committee to ensure that all violations of internal control are reviewed, corrected, and enforced.

Internal control is the company's greatest safeguard against internal theft and embezzlement, and includes the following five components to be effective:

1. The employees are the control environment. Without ethical and competent employees, there can be no effective control. Employees must be part of the process and encouraged to make recommendations.
2. The limits of risk in each area must be evaluated and an acceptable level must be determined.
3. There must be checks and controls in place, such as operating procedures and checklists, to limit risk.
4. The process must be monitored and in an obvious manner. The object isn't to catch a thief but to prevent an employee from having an opportunity to become a thief.
5. The information discovered must be easily and readily available to management for review. Too often weaknesses are discovered but not corrected in a timely manner. This may result in a theft that could have been avoided.

Remember the triangle: pressure, opportunity, and rationalization.

SOX Requirements

The bill further requires that each audit contain an internal control report. This report shall state the following:

1. The responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting
2. An assessment, as of the end of the company's fiscal year, of the effectiveness of the internal control structure and procedures of the company for financial reporting

SOX now directs the SEC to require each publicly traded company, when issuing statements, to disclose whether it has adopted a code of ethics for its senior financial officers and the contents of that code. The SEC was also required to revise its regulations concerning prompt disclosure on form 8-K to require immediate disclosure of any change in, or waiver of, the company's code of ethics.

Reporting on Internal Control

There are two key elements in reporting:

1. The company must assess and report on the company's internal control over financial reporting. This report cannot contain the former get-out-of-responsibility phrase that included the words, "to the best of my knowledge." The statement must not only assess and report its internal control but also be positive. If you find something wrong or inadequate, fix it before issuing the report.
2. External auditors must now audit and report as to the accuracy of management's report. The two audits, financial statements presentation and internal control, must be done at the same time and as part of the same audit because they are so closely related. The audit will, however, be expanded to test the effectiveness of the internal control. This is necessary to evaluate management's assessment.

Impact on Smaller Firms

The impact of SOX on large firms has been very expensive. Its impact on smaller firms will be very expensive and possibly devastating. Several firms have gone private to avoid SOX requirements. Unfortunately, most can't. Many companies fear that this will be their end; they will not survive the cost and will go out of business or start looking to be bought out. It appears that this may be said and done in an attempt to get a change in the law for smaller companies. The PCAOB has stated on several occasions that it is not the intent of the bill to put companies out of business and the extent of the attest need not be so detailed that the bill becomes unmanageable. CPA firms, on the other hand, fear lawsuits or, worse, they fear being banned from audits of public companies. They are not willing to take a chance and refuse to cut back on the audit procedures.

To date, smaller companies have not had to deal with SOX because the compliance date is being extended each time it is about to become effective. There is also talk that the law may be changed after Paul Sarbanes and Mike Oxley retire.

Impact of SOX on the Board of Directors

Audit Committee

Publicly traded companies must have an audit committee on its Board of Directors. Section 301 of SOX establishes general standards of this committee. The audit committee

> … shall be directly responsible for the appointment, compensation and oversight of the work of any registered public accounting firm employed by that issuer (including resolution of disagreements between management and the auditor regarding financial reporting) for the purpose of preparing or issuing an audit or related report, and each such registered public accounting firm shall report directly to the audit committee.

Audit committee members will be members of the board of directors, but in no other way will the issuer or any of its affiliates employ them. They shall be independent. The SEC, however, under special circumstances, exempts members from this rule of serving the issuer in some other capacity.

Each audit committee will have the authority to engage independent counsel and other advisors it determines necessary to carry out its duties. Each company shall provide for appropriate funds for the payment of compensation to any registered public accounting firm employed for the purpose of rendering or issuing an audit report or to any advisors hired by the audit committee under their authority as audit committee. The audit committee shall determine this amount in its capacity as a committee of the board of directors.

The Specialist

Section 407 requires the issuer of the financial statements to disclose in its annual report whether it has at least one audit committee financial expert serving on its audit committee. If the issuer does have a financial expert on its audit committee, they must disclose whether the expert is independent of management.

This financial expert is defined in the bill as an individual who has had, through education and experience as a public accountant or auditor, or a principal financial officer, comptroller, or principal accounting officer of an issuer an understanding of generally accepted accounting principles and financial statements. He must also have experience in preparation or audit of financial statements of comparable issuers

and the application of such principles in connection with the accounting of estimates, accruals, and reserves. He must have experience with internal controls and an understanding of audit committee functions.

The Auditors

External Auditors

All CPA firms auditing publicly traded companies must be registered with the PCAOB. The PCAOB is in turn required to audit the performance of the auditors. Any registered auditing firm auditing more than 100 publicly traded companies a year must be audited every year. All other registered auditing firms must be audited every three years.

The key emphasis on external auditors is independence. This results in the following :

- The audit committee hires the external audit firm.
- The audit firm deals directly with and reports to the audit committee.
- All conflicts over reporting or accounting decisions with management are resolved through the audit committee.
- The auditing firm may perform no other accounting or consulting services other than the audit of financial statements and related audit of internal control and preparation of the federal income tax return.
- The external auditor's partner in charge must change every five years.

Internal Auditors

Internal auditors will no longer report to management but to the audit committee. They may perform audits and assist management in compliance with sections 302 and 404 of the SOX act to the extent that these activities will not interfere with the requirement of the standards for the internal auditor's independence and objectivity.

It is a given that the CEO and CFO will not personally set up internal control procedures, nor will they actually perform the audit of these controls. They will, of course, work with and rely on the expertise of the internal audit department. SOX emphasizes that, although the internal auditor should support management, this work will not interfere with the independence of the internal auditor or his department.

Management

Management has the ultimate responsibility to ensure that proper internal control procedures and philosophy are in place to assure the CEO and CFO that the

financial statements are presented in accordance with generally accepted accounting principles, and that the statements are free of any material misstatements, omissions, or misrepresentations.

Management is further required to communicate to the audit committee and to the auditor all significant deficiencies and material weakness it discovers.

Whistle-Blowers

Encouragement

Whistle-blowing is encouraged. Whistle-blowers are to report to the audit committee any violations of the SOX bill that they observe if, after reporting to and questioning their immediate supervisor, nothing is done.

Protection

In an attempt to protect whistle-blowers, SOX includes the admonition that the company, through policy or any officer, employee, contractor, subcontractor, or agent of the company, should not punish an employee because of any act reported by that employee. This includes, but is not limited to, discharge, demotion, suspension, or in any way discrimination against the employee. Furthermore, anyone who retaliates against a whistle-blower may be fined, or imprisoned for more than 10 years, or both.

Review of Other Highlights of the Act

Signing of Corporate Tax Returns

The Senate included in the bill the phrase, under Section 1001 of the SOX bill, that it was its belief that the federal income tax return of a corporation should be signed by the chief executive officer of the corporation.

Penalties

If a company violates any provisions of the SOX bill, the PCAOB can ban the officers from ever serving on the board of directors or serving as an officer of a publicly traded corporation. This may not sound like much, but to an officer of a large corporation this can result in a sizable cut in pay. In addition to being an officer, most

executives serve on several other boards. Board pay for publicly traded corporations can be sizable.

If the offense is great enough, such as the failure of corporate officers to certify financial reports, the fine can be as high as $5,000,000, or 20 years in jail, or both. In addition, many officers are being required to pay back bonuses and profits made from fraudulent transactions they were responsible for, such as, but not limited to, overstating sales and receivables, classifying expense as an asset to inflate profit, or gain on insider sale of stock.

The penalties for defrauding shareholders of a publicly traded corporation are punishable by fines, or imprisonment for a period not to exceed 25 years, or both.

Section 404

Section 404 is a very short section of the bill and is creating the major concern and expense. In establishing the requirement for internal control, the PCAOB requires that the report of CEO and CFO of a publicly traded company provide the following:

1. State the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting.
2. Contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

In addition to this, Section 404 requires the following:

> Each public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer.

With no guidance from the PCAOB as to the extent of the examination required by management or the audit firm, both sides were at a loss.

- Management was not sure about the extent and detail that they must audit internal controls. For a multinational conglomerate, it is impossible to visit all the sites, let alone review the internal control procedures. They must assure themselves that the philosophy of the company is reflected in the understanding of the employees, and in the internal control guidelines and monitoring of the internal control auditors and managers. But how much detail is enough?
- External auditors have the same problem. They worry about being sued if they do not delve into enough detail to assure themselves that their audit is complete enough and that they have reviewed enough to assure themselves that

> they agree with management. Unfortunately, the fear is creating an extremely large auditing fee, which was not the intent of the bill.

In conclusion, the Sarbanes–Oxley Bill of 2002 has brought to light areas of concern regarding internal control and potential disaster from within for many companies. Internal control has always been an area of great concern and potential loss.

Theft has been recorded by some companies by setting up cameras in the factory and on the loading docks and parking lots. They film employees carrying merchandise out of the manufacturing plant and loading it into their cars. Later they hold a staff meeting for all of the thieves, show them the film, and open the doors for the police to enter and arrest them. They then march them through the plant in handcuffs to the waiting police vans. This could never happen if internal control procedures for supervisors were being enforced.

Internal control efforts can be as simple as a publicly traded company deciding to conform to federal law and send out 1099s to vendors. In doing so one company discovered that a vendor in Chicago was receiving checks sent to a Dallas address and that he had received in Dallas three times the amount that was sent to Chicago. Had the finance director looked at the pay vouchers and backup as a part of the internal control procedures, this could never have happened. But he was a trusted employee who embezzled over $600,000.

Sadly, there are also the cases where lack of internal control or internal control enforcement has sent companies to the bankruptcy court.

SOX, however, was designed to go after the unethical executives. Unfortunately, at this stage of their life they are either ethical or not; it is too late to teach them ethics. Instead, Congress imposed penalties — penalties that we have discussed earlier. It was their hope that the fear of going to prison or the fear of up to a $5,000,000 fine might be sufficient. Additional penalties may include not allowing the executive from serving on the board or as a corporate officer of a publicly traded corporation.

This may look like something that is beyond your control. You can't control the ethics of your employer. That brings us back to the whistle-blower provision of the bill. These facts need to be taken directly to the audit committee. They want to know these facts because they may be held responsible and may be fined or given jail time because they should have known these facts. There might still be an Arthur Anderson or WorldCom today, had this bill been in effect then.

Special Additional Section: Regulatory Issues and How They Affect Business Continuity (BC) Programs

Tracy Cowan
Rick Holler

Mandates/Legal Requirements

- What is a legal requirement?
- Statute — legislative action
- How do you identify these?
- Research is available

Hooper Doctrine

- This doctrine establishes that "precautions are so imperative that even their universal disregard does not excuse their omission."
- As a defense, a company cannot use the fact that there are no specific requirements to have disaster recovery plans because they know other companies do not have them.

Sarbanes–Oxley (SOX)

- Corporate reform legislation for financial accountability.
  - Passed because of high-profile accounting irregularities.
- GOAL: To make companies (executives) more accountable and to protect the shareholders

SOX Law in effect as of July 30, 2002

Section 302:

CEO/CFO certify financial reports and internal controls: August 29, 2002

Section 304:

CEO/CFO subject to compensation, forfeiture, and penalty when accounting restatements due to material noncompliance and misconduct occur

Section 404:

- SEC Reporting Companies — $75M+: June 15, 2004
- SEC Reporting Companies — periodic reporting: April 15, 2005
- SOX affects public companies, and some private companies have activities that would fall under these regulations.
  - Board of Directors (BOD) representing Shareholders
  - Public Offerings
  - Partners with public companies
  - Reality is that many private companies will be affected
- BC programs: Sections 302, 304, and 404 directly require a company's ability to exhibit a high regard for financial reporting.
  1. Establishing the necessary internal controls covers the following activities:
     - Control environment
     - Awareness
  2. Risk assessments
     - Identification and analysis of internal/external risks
     - Manage/mitigate risk through controls
  3. Control activities
     - Establish and enforce policies/procedures
     - Should include backup and recovery strategies and ensure recovery plans are in place
  4. Information and communication
     - Information processes from a BCP perspective includes:
       a. Performing a business impact analysis (BIA)
       b. Performing backups
       c. Creating a recovery strategy
       d. Creating a BC plan
  5. Monitoring

- Process that assesses the quality of an organization's internal controls performance
  a. Periodic BC testing will validate this quality and accuracy of data, records, and recovery processes

Health Insurance Portability and Accountability Act (HIPAA)

- Created in 1996
- Regulates electronic security and transmission of patients' records
- Requires healthcare organizations to produce well-documented and updated recovery plans for:
  - Computer systems
  - Software applications
  - Advanced medical technology
- HIPAA is complemented by the Joint Commission on the Accreditation of Healthcare Organization (JCAHO)
  - JCAHO regulations require that all hospitals MUST have an emergency management program so that patient care can be continued effectively in the event of a disaster.
  - CAHO requires hospitals to conduct disaster drills twice a year, at a minimum.
- Patient care is the primary focus when initiating business continuity into a healthcare system.
- Healthcare operations must be well coordinated:
  - IT management
  - Business continuity planners
- An effective BC program helps to determine which departments have documented work-around procedures.
- Plans need to include prioritization procedures for moving any patient's care to another healthcare facility.

Gramm–Leach–Bliley Act

- Effective 1999 — known as the Data Protection Rule
- Requires federal banking agencies "to consult with one another to establish consistent and comparable standards for financial installations to safeguard all customer information." These include:
  - National Credit Union Administration
  - Securities and Exchange Commission

  - Secretary of the Treasury
  - Federal Trade Commission
- Broad enforcement measures include:
  - Corrective actions
  - Fines
  - Penalties
  - Audit continually for compliance
  - Applies to all vendors and service providers that deal with transactions or processing customer data.
- Business requirements include:
  - Identify risks.
  - Form a strategy to manage risks.
  - Implement the strategy.
  - Test the implementation.
  - Monitor to control identified risks.
- Auditors specifically look for:
  - Documented policies
  - Business contingency plans
  - Evidence of general testing
  - Implement corrective actions
  - Assessments on preparedness for third-party providers

Federal Financial Institution Examination Council (FFIEC) Thrift Bulletin 30

- Effective July 1989 — Supersedes R67.
- BC Program: Requires institutionwide contingency planning.
- Perform a risk assessment:
  - Physical
  - Operational
- Evaluate critical needs and priorities to determine recovery strategies.
- Ensure written plans are tested and reviewed, and maintain regularly.

References

Computer Security Act — http://www.house.gov/science/hr1903.html.
FDIC FIL-68-97 — http://www.fdic.gov/news/news/financial/1997/fil9768.html.
FFIEC Information Systems —
http://www.ffiec.gov/ffiecinfobase/html_pages/bcp_book_frame.htm.
http://www.ncua.gov/ref/ffiec/vol2bm.pdf — Volume 2.
http://www.fdic.gov/regulations/information/information/s3c29.pdf.
Rule 447 — NYSE.

Foreign Corrupt Practices Act — http://www.usdoj.gov/criminal/fraud/fcpa/.
HCFA- HIPAA Regulations — http://www.hcfa.gov/hipaa/hipaahm.htm.
ISO Qualifications — http://www.iso9000.org/.
OCC 97-23 FFIEC Interagency Statement on Corporate Business Resumption and Contingency Planning — Policy Statement Revision 5/16/97 — http://www.occ.treas.gov/ftp/bulletin/97-23a.pdf.
Paperwork Reduction Act of 1995 — http://www.hcfa.gov/regs/prdact95.htm.
Richmond — Federal Reserve BC Plans — http://www.rich.frb.org/banking/dig/.
http://www.ncua.gov/ref/ffiec/vol1bm.pdf — Volume 1.

Appendix 1

Now Pull It All Together and Write a Great Disaster Recovery Plan

Leo A. Wrobel

Business Continuity and Disaster Recovery Plan for

_____

_____

_____

Confidential

FILL IN YOUR COMPANY NAME HERE
Business Continuity and Disaster Recovery Plan

Contents

Introduction Section

This is the section where you will write the Executive Summary or Mission Statement previously discussed. Central themes include:

- Protect lives
- Minimize risks

- Recover critical operations
- Protect against lawsuits
- Preserve competitive position
- Foster customer confidence and goodwill
- Overview of recovery strategy

All in One Page or Less

Take a shot at writing your Executive Summary on the following page. You might want to consider doing this last.

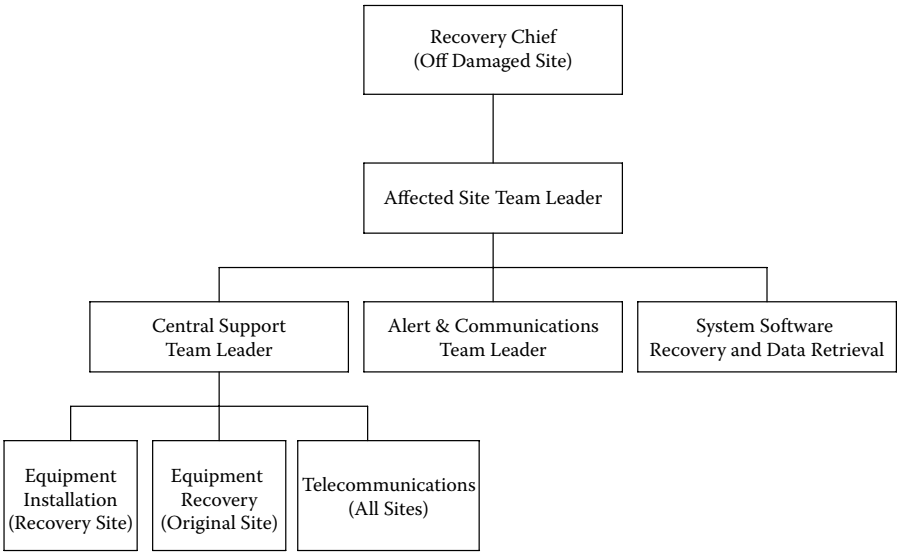


Figure A1.1 Disaster recovery organization.

EXECUTIVE SUMMARY

Goals

Protect lives _____

_____

Minimize risks _____

_____

Recover critical operations _____

_____

Protect against lawsuits _____

_____

Preserve competitive position _____

_____

_____

Foster customer confidence & goodwill _____

_____

Overview of how we will do it _____

_____

_____

Briefly fill in the blanks above, then turn over to a good "wordsmith" to finalize the document.

One picture speaks a thousand words (see Figure A1.1). By using diagrams like this one, someone who is not you can instantly see the game plan. Write for your audience.

	Audience		*Mode of Presentation*
✓	Management	✓	Organization
✓	Programmers	✓	Flowcharts
✓	Technicians	✓	Schematic diagrams

Scope

This Technical Services Disaster Recovery Plan is designed to respond to a disaster in a _____ Equipment Room, equipment room, or other facility under the oversight of the Information Technology function. A disaster is defined as an incident that damages the facility, equipment, or data, supporting a "mission-critical" business function. The plan provides the recovery tasks, checklists, forms, and procedures required to allow assigned personnel to effect a timely recovery.

Organizational areas covered in this plan include:

- Support for MIS restoration or relocation.
- Support for internal systemwide outages, such as Equipment Room and PBX failures.
- Support for public telecommunications carrier failures or sabotage.
- Other specific items

Notes:

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Here is an example of the Scope section. Use the verbiage above for your plan, and add items relevant to your organization in the Notes section above. You have just begun documenting your plan!

Objectives

The Disaster Recovery Plan is designed to accomplish the following objectives:

- Identify and staff disaster response teams for emergency recovery functions.
- Train and prepare personnel to respond to disasters.
- Coordinate disaster recovery activities between _____ divisions.
- Promptly restore essential information services to _____ facilities in alternate work locations, if necessary.
- Repair, replace, or restore equipment at the damaged site.
- Maintain effective command and control in any recovery effort.

This document is designed to provide for an organized recovery from major disruptions, with a minimum of interruption to business and operational services. Portions of this plan were adapted from other _____ recovery plans, such as Plant Engineering, to allow for standardization and greater interdepartmental continuity.

Notes:

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Here is an example of the Objectives section. Use the verbiage above for your plan, and add items relevant to your organization in the Notes section above.

Plan Overview

- The plan specifically identifies key "Department" personnel and their recovery responsibilities. The recovery assignments are listed on the Disaster Recovery Organization Chart shown on the first page of this section.
- Disaster Recovery Plan activities are initiated through a First Alert process. Management is informed of a disaster at a facility immediately after discovery of the situation.
- An Initial Assessment of the damage will be made. The location of a Recovery Headquarters will be selected.
- Recovery Management will assess the situation and determine if there is a need to activate the Disaster Recovery Plan.
- If the situation warrants full activation of the plan, procedures identify authorization responsibilities and activation steps. This is explained in the site-specific alert procedures beginning in section ____.
- Individuals will be assigned to designated recovery tasks and participate in specific recovery teams.
- The Recovery Plan is divided into two categories:
  A. Operating and Security Standards (Appendix ___)
  B. Recovery Procedures (the remainder of the document)
- Certain checklists are also provided where recovery tasks require a check-out column. These can be found in the appendix section at the back of this plan. Forms are sometimes included that provide control mechanisms for recovery activities after the plan is activated.
- In some instances, where the required information is complex, reference is made to where the information can be obtained from an external source, such as a company policy. This is called a "pointer."
- Existing reporting relationships will change during a recovery operation to provide central recovery direction and control. These reporting changes are documented in the plan.

Notes:

_____

_____

_____

_____

Here is an example of the Plan Overview section. Use the verbiage above for your plan, and add items relevant to your organization in the Notes section above.

- Certain checklists are also provided where recovery tasks require a check-out column. These can be found in the appendix section at the back of this plan. Forms are sometimes included that provide control mechanisms for recovery activities after the plan is activated.
- In some instances, where the required information is complex, reference is made to where the information can be obtained from an external source, such as a company policy. This is called a "pointer."
- Existing reporting relationships will change during a recovery operation to provide central recovery direction and control. These reporting changes are documented in the plan.
- The plan makes provisions for establishing a Recovery Headquarters. The Recovery Headquarters is the "meeting place" from which essential recovery activities are coordinated. The Recovery Headquarters Staff will alert all Information Technology, MIS, and other personnel of the disaster and will notify users concerning the service impact. This group will provide all administrative and clerical support, coordinate travel arrangements, and establish a method to handle incoming telephone calls and media inquiries. It will collect all recovery status and expense reports. Also, this group will coordinate initial data retrieval activities from the off-site storage location.

The plan makes provisions for restoring damaged equipment. An Equipment Room Restoration team coordinates the damage assessment and restoration tasks for the facilities, equipment, data, forms, and supplies.

Notes:

_____

_____

_____

_____

_____

_____

_____

_____

_____

Here is an example of the Plan Overview section. Use the verbiage above for your plan, and add items relevant to your organization in the Notes section above.

The Systems Software team coordinates the recovery tasks for restoring LANs, mainframe, and telecommunications software.

The Wide Area Network Configuration section details the recovery tasks for providing physical network transport services immediately following a disaster situation to the local telephone company or IXC (long distance carrier), including:

- Loss of IXC (interexchange carrier) such as AT&T.
- Loss of AT&T C.O.
- Loss of major _____ communications hub.

Notes:

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Here is still another example of the Plan Overview section. Use the verbiage above for your plan, and add items relevant to your organization in the Notes section above.

Disaster Scenario

The Technical Services Disaster Recovery Plan has been designed to respond to the situation where a disaster occurrence prevents the delivery of mission-critical information services for an unacceptable period of time. "Critical" and "unacceptable" are relative terms that can only be quantified by company management based on an analysis of financial impact and degradation of customer service.

Disasters include (but are not limited to):

- Fire and explosion — intentional/accidental
- Water damage — Overhead leakage, sprinklers, etc.
- Acts of God
  - Floods
  - Earthquake
  - Hurricane
  - Tornado

Notes:

Here is an example of the Disaster Scenario section. Use the verbiage above for your plan, and add items relevant to your organization in the Notes section above.

Exclusion from computer site:

- Terrorist takeover
- Bomb threat
- Rioting, martial law
- Compromise of structural integrity
- Contamination, causing abandonment of structure

It is also important to note that unlike more "traditional" recovery planning (as for mainframes), the focus of concern has sometimes shifted. Whereas in mainframes we have been mostly concerned with what can happen "in here" (the computer room), with open systems, telecommunications, and the prospect for terrorism, for example, we are most concerned with what can happen "out there" (the network). The plan considers these new dynamics.

Disasters in open systems can also be particularly serious, because open systems are often directly tied to the core business; the revenue impact is immediate.

Notes:

Here is a continued example of the Disaster Scenario section. Use the verbiage above for your plan, and add items relevant to your organization in the Notes section above.

General Recovery Strategy

20.01 Recovery Strategy

The primary objective of the information technology recovery teams will be to concentrate efforts on reestablishing mission-critical information services in an affected facility as indicated by the situation. Salvageable items will be restored, whereas those irreparably damaged will be quickly replaced by means of "rapid replacement" vendor programs, equipment restoration companies, relocation of the department, or other methods. The following section details the specific individual responsibilities to ensure an orderly recovery process.

Notes:

Recovery Teams

20.02 Formation of Recovery Teams

20.02.01 The Executive Management Team (EMT)

During any possible disaster in a _____ facility that may have affected an automated system (meaning open systems, mainframes, telecommunications, etc.), a core contingent of its employees will assemble for the purpose of coordinating the disaster response. These employees are referred to as the Executive Management Team, or EMT. Detailed duties and responsibilities of the EMT are contained in Appendix 1 of this document.

20.03_____ Executive Involvement in the EMT

In the event the disaster causes a major disruption in production, cash flow, normal public relations, or other situation requiring executive involvement, selected _____ executive personnel will also become involved. These persons and situations are contained in the operating standards in Appendix 18.

20.04 First Alert Procedures

First Alert procedures are defined in Section 30, and are designed to ensure that word gets out from those persons who will probably first discover the disaster (Plant or Building Engineering) to the Information Technology Team, which will respond.

20.05 Initial Response Personnel

Information Technology personnel to respond to a possible disaster will include:

The Executive Management Team
The Affected Site Team Leader
Central Support Coordinator
Data Retrieval Leader
Equipment Installation Team Leader
Equipment Recovery Team Leader
Systems Software Manager

20.06 Response Personnel — Outlying Plants

(On-site personnel in the outlying plants are identified in Appendix 13.)

Notes:

Notification Procedures

30.00 Specific Recovery Notification Procedures

30.01 Locations Affected

The following locations are deemed critical to the operation and continuance of _____ business activity and have special procedures for restoration outlined in this document. They are also the direct responsibilities of _____

List Your Locations Here

_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

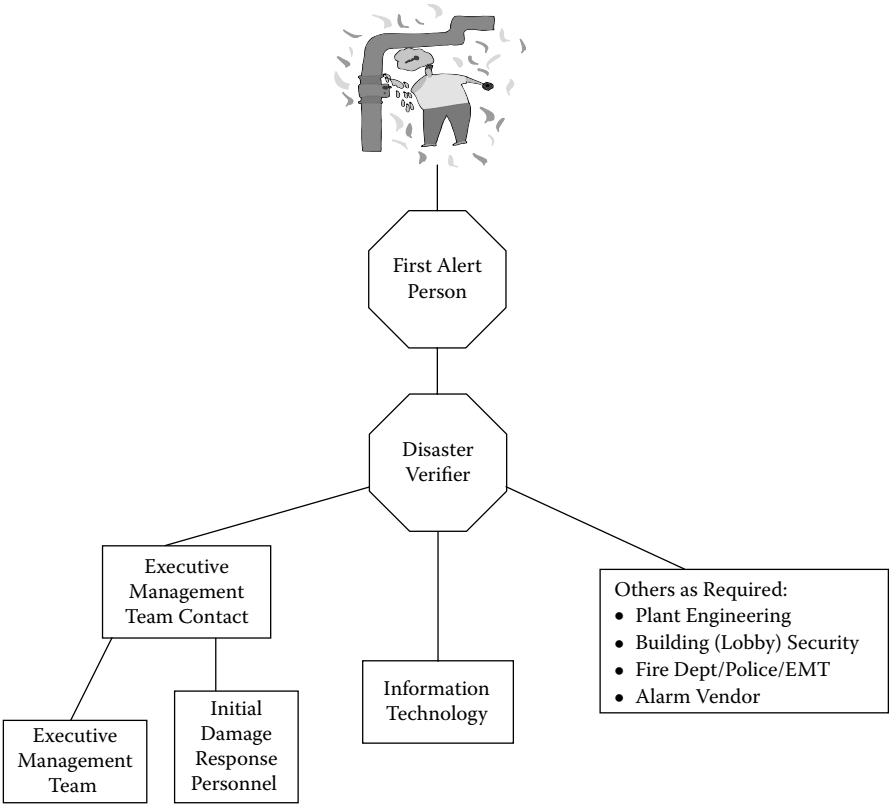


Figure A1.2 "First alert" procedures.

1. Event occurs, such as broken water pipe at 3:00 A.M.
2. First Alert person notices and reports the incident to Plant Engineering.
3. The responsible plant engineer receiving the report becomes the Disaster Verifier.
4. The Disaster Verifier notifies other departments, including Information Technology.
5. If the situation warrants, a disaster is declared.

Procedures are included in this section.

30.02 What to Do If You Are the First Alert Person

If you are the first person to become aware of a problem at the building, assume **First Alert Person** responsibilities.

1. Immediately after completing the alerts and notifications required by existing emergency procedures, determine whether the disaster could have affected computers, telecommunications, or other specialized equipment.
2. If the electronic equipment could have been affected, notify one of the Initial Disaster Response Personnel listed in Appendix 13 of this document. Use the form below to log each name, the time you called them, and the outcome of the call.

NAME	*HOME PHONE #*	*RECORD OUTCOME OF CALL*

Furnish the following information to the first individual contacted:

1. Your name
2. Phone number where you can be reached
3. Description of the disaster occurrence
4. Preliminary report of damages and injuries
5. Any information regarding attempted or actual contacts from #2 above

Notes:

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

30.3 What to Do If You Are the Disaster Verifier

1. The first person contacted and notified of the disaster will assume the responsibility of the Disaster Verifier and perform all the tasks outlined below.
2. While on the telephone with the First Alert Person, obtain information related to the following questions (use form below):
   a. Who is raising the alarm?

      Name: _____

      Time: _____

      Date: _____

      Day: _____

      Contact phone: _____

      Location: _____

Notes:

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

b. What is the nature of the problem?_____
What is the preliminary assessment (damages and injuries)?

_____

_____

_____

c. Can access to the building be gained?_____

_____

d. Are there any immediate dangers or restrictions? _____
e. Review status of contact attempts. _____
f. Provide information as to when you will arrive and where you will meet the first alert person.
g. Advise first alert person that you will make all contacts.
h. Remind first alert person not to make any public statements regarding the situation.

Notes:

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Verify that a disaster situation exists by calling one of the following:

	PHONE NUMBER	*OUTCOME OF CALL*
Information technology		
Plant engineering		
Building security (lobby)		
Guard shack		
Fire department Dispatcher		
Police department dispatcher		
Alarm vendor		
Emergency services	911	

Note: If verification telephone contact cannot be established, assume disaster mode and proceed with the disaster verification responsibilities.

Notes:

*Guard desk _____

*Telephone room _____

*Office areas _____

*Nearest pay phones _____

*Location _____

Telephone numbers that are operational during extended power outages up to 4 hours are listed in Appendix __. Use these numbers if the disaster makes normal phones inoperable. Use form above to write down the numbers you are using.

Notes:

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Notify one of the Executive Management Team personnel from Appendix 1 of this plan that a disaster situation exists. Use the Personnel Notification Procedure — Appendix 13. This person will become the Executive Management Team Contact. Start with the Recovery Chairman; if unavailable, go down the list in order as shown in Appendix 1.

Title/Team	*Person Contacted*	*Home Phone*	*Time Contacted*	*Result of Contact*
EMT				
Affected Site Team Leader				
Central Support Team Leader				
Data Retrieval Leader				
Equipment Installation Team Leader				
Equipment Recovery Team Leader				
Systems Software Manager				

Notes:

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

1. Provide the following:
   a. Preliminary assessment information.
   b. Status of all contacts.
   c. Name and contact phone number of the individual making the FIRST ALERT.
   d. Estimated time of your arrival at the disaster site.
   e. Estimated time elapsed for a follow-up call with instructions related to activation or cancellation.
   f. Instruct the Executive Management Team Contact to prepare for Executive Management Team and Company Management Alert.
2. Take your copy of the Disaster Recovery Plan, travel to the disaster site, and contact the following individuals upon your arrival:
   First Alert individual
   a. On-site company building management personnel
   b. On-site company security personnel
   c. On-site fire/police captain
3. Obtain the following information:
   a. Can the facility be entered?

      _____

   b. If not, when will access be allowed?

      _____

      _____

      _____

   c. Estimate of damage to the building:

      _____

      _____

   d. Estimate of damage to the contents:

      _____

      _____

   e. Estimate of damage to the computer equipment:

      _____

      _____

4. Make no public statements regarding the situation or use a general statement.
5. If the facility can be entered, tour the area and evaluate the extent of damage.
6. Evaluate all information obtained and decide if a true disaster situation exists. If all facilities, equipment, and data are unaffected and the problem can be

easily solved by operations personnel and vendor systems engineers, notify the Executive Management Team Contact to cancel all Disaster Recovery Plan Activation activities.

7. If a disaster situation does exist: Select the location for the Recovery Headquarters.
   a. The affected facility (if accessible) is the first choice.
   b. Second choice — _____
      Large 1st Floor Conference Room
      2450 Preston Rd.
      Dallas, Texas 75235
      Phone: (214) 555-7602
   c. Third choice — As directed by Recovery Chairman.
8. Notify the Executive Management Team Contact to proceed with the Executive Management Team and Company Management Alert.
9. Assist in establishing an area to house the news media in the vicinity of the affected facility.
   a. Direct news media to the assigned area.
   b. Provide news media with the following initial statement:

Notes:

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

MEDIA AFFAIRS

Avoid panic among families, investors, and media. Develop a solid press release in advance of a disaster and include it in your plan.

Initial News Media Statement

The emergency is being handled in accordance with established company emergency procedures. Our management team is meeting with the local authorities right now to obtain official information related to the incident.

a. We want you to publicize the facts regarding the situation.
b. Management will be presenting a company statement very shortly. You will be invited and advised of the location … ”
c. The situation is under control.

Notes:

_____ Press Release

"_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____"

Take a shot at your own press release here. Better yet, have someone in your legal department do it.

WHAT DOES THE EMT DO?

30.04 What to Do If You Are the Executive Management Team Contact

The Executive Management Team will be assembled only when authorized by an Executive Management Team member contacted by the damaged site.

1. Determine and write down the following information prior to making calls:
   a. Headquarter's location _____
   b. Headquarter's telephone #_____
   c. Name of Executive Management Team Members at disaster site _____
   _____
   d. Brief description of problem _____
   _____
   _____
   _____
2. Travel to Recovery Headquarters.
3. Alert all Executive Management Team members that a disaster situation exists and direct them to report to the Recovery Headquarters. Use the Personnel Notification Procedure in Appendix 13. Use the form below to log the status of your efforts.

Name	Phone Number	Outcome of Call

Notes:

_____

_____

_____

30.05 Disaster Assessment/Plan Activation

When the available Executive Management Team members assemble at the Recovery Headquarters, they will direct the following activities:

1. Dispatch several Executive Management Team members to the disaster site to reassess the extent of damage to the facility and its contents. Instruct the individuals to:
   a. Tour the affected area if access is allowed.
   b. Obtain facility and content damage reports from on-site management or local authorities.
   c. Obtain injury reports from on-site representatives or local authorities.
   d. If access is restricted, obtain an estimate of when access will be allowed by local authorities.
   e. Formulate a Disaster Recovery Plan Activation or Cancellation recommendation.
2. Set up a Command Center at the Recovery Headquarters to:
   a. Review the findings of the re-assessment activities.
   b. Answer telephone contacts and provide a focal point for Command and Control.
   c. Determine the level of disaster:
      i. Limited Recovery — Only certain teams may be activated based on the affected areas. The potential types and duration of instances requiring Limited Recovery are numerous, but could include loss of a LAN or PBX system, with the rest of the building intact.
      ii. Long-term Recovery — This level of disaster may require that all teams be activated (LAN, Telecom, Facilities, Plant Engineering, Executive, etc.). The goals and objectives of the recovery operation have been identified and each team's specific activities will be controlled by the recovery tasks within the plan.
   d. Review the recommendations to Activate or Cancel.

Notes:

_____

_____

_____

_____

_____

_____

3. If no further recovery activities are required, Cancel all recovery activities.
4. If recovery operations are required, obtain approval to activate the plan. Only the Executive Management Team or the designated alternate is Authorized to activate the Disaster Recovery Plan. In the absence of both individuals, a designated _____ officer-level executive will activate and coordinate the plan.
5. Authorize Activation of the Disaster Recovery Plan throughout the affected area.
   a. Identification of the recovery goals and objectives.
   b. Identification of any additional individuals or support teams required at the Recovery Headquarters and authorization for the alerting of those persons (use form on next page).
6. Alert all remaining assigned personnel, and instruct them to report to the Recovery Headquarters.
7. Advise senior management and Information Technology executives at corporate telecommunications that the plan has been activated; request that they advise their staff members.
8. Contact and alert utility services using form at the end of this section.

Name	*Title*	*Phone Number*	*Outcome of Call*

(All area codes are _____ unless otherwise noted.)

Notes:

_____

_____

_____

_____

_____

_____

_____

_____

30.06 Recovery Team Alert Checklist

The Executive Management Team will use the checklist below to alert remaining managers and Function leaders and to make appropriate alternate assignments. Highlight the actual individual responsible during recovery. See Appendix 13 for telephone numbers.

Distribution Register

The following outline identifies the primary and alternate areas of responsibility for the Staff Support individuals/departments for the Disaster Recovery Plan.

Function	*Person Contacted/ Number*	*Result of Call*
Corporate Communications		
Human Resources		
Facilities		
Finance		
Risk Management		
Internal Audit		
Labor Relations		
Legal		
Medical		
Office Services		
Public Affairs		
Purchasing		
Transportation		
Telecommunications		

Use a Utility Service Checklist similar to the following.

UTILITY SERVICES

30.07 Utility Services Alert Checklist

Commercial Utility Services Alert Checklist

Utility Company:
Electric and illuminating — Name: _____
Business # _____
Service telephone #: _____
Type of service: Electric — Result of alert: _____

Utility Company:
Water department — Name: _____
Business #: _____
Service telephone #: _____
Type of service: Water — Result of alert: _____

Utility Company:
Gas — Name: _____
Business #: _____
Service telephone #: _____
Type of service: Gas — Result of alert: _____

Notes:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

RECOVERING OPEN SYSTEMS (LANS)

40.00 LAN Restoration or Reconfiguration

Add a high-level overview for restoration of your organization's "open systems" here.

Notes:

Refer back to your checklists of "top ten" mission-critical systems from Chapter 1.

TELECOMMUNICATIONS RECOVERY

50.00 WAN Recovery

Add references to your firm's telecommunications procedures here.
Don't forget:

- Redirection of incoming numbers
- Publication of EMT numbers
- Wireless numbers of key employees

50.05 Customer Notification Procedures

50.10 Redirection of Dial-in Maintenance Ports

50.15 IP Network Reconnection and Establishment

50.20 Router Network Reconnection and Establishment

50.25 PBX, ACD, and Voice Mail Disruption

50.30 Emergency Carrier Override Procedures for Long-Distance Company Failure

50.35 800 Service Redirection/Restoration Procedures

50.40 AT&T Call-Forwarding and Redirection Procedures

50.45 Equipment Software Load/Remote Load Procedures

Other Systems (List here)

_____

_____

_____

_____

NOTIFYING YOUR INTERNAL CUSTOMERS

Customer Notification Procedures

Notes:

_____

_____

_____

_____

_____

Redirection of Dial in Maintenance Ports

Notes:

_____

_____

_____

_____

_____

IP Network Reconnection and Establishment

Notes:

_____

_____

_____

_____

_____

Router Network Reconnection and Establishment

Notes:

_____

_____

_____

_____

PBX, ACD, and Voice Mail Disruption

Notes:

_____

_____

_____

_____

Emergency Carrier Override Procedures for Long-Distance Company Failure

Notes:

_____

_____

_____

_____

800 Service Redirection/Restoration Procedures

Notes:

_____

_____

_____

_____

AT&T Call-Forwarding and Redirection Procedures

Notes:

_____

_____

_____

_____

Equipment Software Load/Remote Load Procedures

Notes:

_____

_____

_____

_____

RECOVERY TEAMS

- What?
- Why?
- Who?

Executive Management Team

What?

- Report immediately to Recovery Headquarters.
- Provide liaison to senior management, request executive representative if necessary.
- Authorize Recovery Plan Activation.
- Provide high-level management and coordination of the recovery process.
- Review reports submitted by:
  - The EMT
  - The Affected Site Team Leader
  - Central Support Coordinator
  - Data Retrieval Leader
  - Equipment Installation Team Leader
  - Equipment Recovery Team Leader
  - Systems Software Manager

Why?

- Compile report for executive management based on input reports from teams.
- Maintain interface with staff support department representatives.
  a. Legal
  b. Facilities
  c. Purchasing
  d. Risk management
  e. Security
  f. Transportation

Who?

Generally executive management

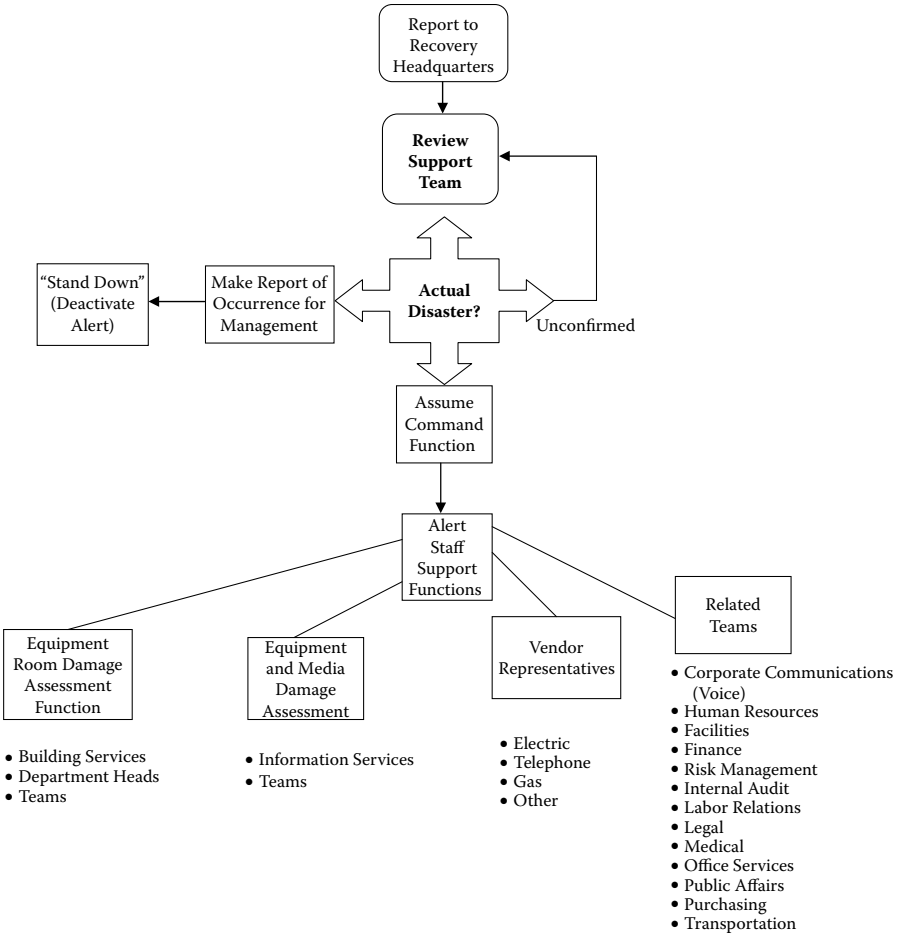


Figure A1.3 EMT duties and responsibilities.

Who?

Responsible Individuals Fill in Their Names Here

Department	*Primary/Alternate*	*Home Phone*	*Result of Alert*
EMT			

Affected Site Team

What?

Maintain security and begin restoration of the damaged site.

Why?

1. Report immediately to damaged site.
2. Direct initial assessment activities.
3. Alert Staff Support Department management.
4. Direct recovery operations, including:
5. Direct damage assessment activities (repairs and replacement).
6. Activate Equipment Room Restoration functions as required.
7. Monitor Equipment Room Restoration activities.
8. Determine the extent of damage to:
   a. Equipment (LANs, voice and data communications)
   b. Data and magnetic media
   c. Documentation (paper)
   d. Forms
   e. Other
9. Evaluate salvageable status with vendor (Call BMS Catastrophe, for example).
10. Coordinate move and storage of salvageable items.
11. Determine need to order equipment.
12. Coordinate ordering and receipt of replacement equipment and material.
13. Monitor the repair of damaged equipment.
14. Coordinate the installation and testing of equipment.
15. Coordinate movement of personnel, equipment, and material to alternate site.

Who?

16. Obtain the names of the Staff Support Department representatives from the Recovery Headquarters Manager. The representatives will support damage, salvage, and restoration activities.

Staff Support Department	*Name*	*Number*
Security		
Facilities		
Risk management		
Purchasing		
Legal		
Transportation		

17. Maintain good written documentation of all changes and modifications to current operating procedures in anticipation of return to normal operations.
18. Maintain a record, with receipts where possible, of all personal expenses incurred during the recovery operation.
19. Accumulate daily written Recovery Status Reports from the assigned Subordinate Team Leaders; prepare an overall report and forward to the Recovery Headquarters Manager.
20. Accumulate all Expense Reports, from the assigned Subordinate Team Leaders; review, approve, and submit to the Recovery Headquarters Manager for processing.

Who?

Responsible Individuals Fill in Their Names Here:

Department	*Primary/Alternate*	*Home Phone*	*Result of Alert*
Affected site team			

Notes:

_____

_____

_____

Central Support Team

What?

Provide for the care and feeding of the EMT.

Why?

1. Report immediately to Recovery Headquarters.
2. Ensure that adequate space and facilities are provided in Recovery Headquarters.
3. Conduct an initial meeting with the assigned personnel.
4. Review incoming status reports on the condition of the facility and its contents. Keep the Affected Site Team Leader informed on all team status reports and restoration recommendations.
5. Alert the major vendors regarding the situation and request their assistance. Provide the vendor names to the Affected Site Team Leader so that temporary passes can be issued to help control site access.
6. Distribute inventory lists to the appropriate recovery function leaders for damage assessment and salvage activities. These are included in this plan under the following sections:

Title	*Section #*
Equipment inventory	Appendix __
Forms inventory	Appendix __

7. Request assistance from the utility companies, if required, to assess damage and restore services. Use the Utility Services Alert Checklist. Obtain clearance to send personnel into the affected building. Obtain the approval from an authorized individual (Facilities, Security, or local authorities). To protect the company from a possible negligence suit, obtain a written access authorization, if possible.
8. Activate an Equipment Room Damage Assessment function (if not already done), and direct recovery personnel to travel to the disaster site and initiate facility damage assessment activities.
9. Obtain a facility damage assessment report from the Equipment Room Damage Assessment Leader and promptly notify the Affected Site Team Leader about the status of the damaged facility.
10. Activate an Equipment/Media Damage Assessment and Salvage function and direct recovery personnel to travel to the disaster site to initiate salvage activities.

11. Obtain a salvageable data report from the Equipment/Media Damage Assessment and Salvage Leader. Promptly notify the Affected Site Team Leader of salvageable data.
12. Using the list of salvageable equipment obtained from the Equipment/Media Damage Assessment and Salvage Leader, develop purchase orders for required replacement equipment.
13. Obtain appropriate approvals and coordinate the ordering of replacement equipment.
    a. Maintain lists of ordered equipment.
    b. Designate space for delivery, acceptance, and temporary storage.
    c. Establish procedures to control the delivery, receipt, and storage of equipment.
    d. Maintain accurate records of equipment ordered and received.
    e. Maintain a record of any extraordinary charges resulting from equipment delivery or storage.
    f. Provide copies of all invoices to the Affected Site Team Leader.
14. Obtain estimated delivery dates from the vendors for replacement of equipment. When required, meet with vendor senior management to expedite shipments of equipment.
15. Review and approve restoration recommendations.
16. Act as an interface between the Executive Management Team, the Risk Management representative, and the insurance company.
17. Act as an interface between the Executive Management Team and all departments, contractors, and vendors regarding assessment, salvage, and reconstruction activities.
18. Be prepared to meet with the Executive Management Team and other senior management personnel to provide status reports and recommendations on repair and reequipping activities.
19. Monitor all facility construction, repair, or selection activities with the appropriate staff representatives.
20. Direct and monitor all Equipment Room Restoration activities for the duration of the recovery operation.

Who?

Selected responsible executive support staff personnel.

List Responsible Individuals' Names Here:

Department	*Primary/Alternate*	*Home Phone*	*Result of Alert*
Affected site team			

Notes:

_____

_____

_____

_____

Facility Restoration Team Organization

Affected Site Team Leader

Equipment room damage assessment function
Equipment/media damage assessment and salvage function
Vendor representatives
Liaison with related teams

Notes:

_____

_____

_____

_____

Related Team Support Checklist for Central Support Function

Use this checklist to determine where staff support is required. The predetermined recovery support functions are listed below. An "X" identifies the areas requiring support representatives. Once you have determined the needs based on the situation, provide the names and functions to the Damaged Site Team Leader so that he or she may make arrangements for support.

Support Function	*Recovery Headquarters*	*Affected Site*
Employee Relations	X	
Facilities	X	X
Finance	X	
Risk Management	X	
Internal Audit	X	
Labor Relations	X	
Legal	X	
Telecommunications	X	X
Office Services		
Mail Services	X	
Security	X	X
Shipping & Receiving	X	X
Medical	X	X
Public Affairs	X	X
Purchasing	X	
Transportation	X	

Equipment Installation Team (Recovery Site)

What?

Installation of new equipment at backup location.

Why?

1. Report immediately to computer recovery facility or as directed.
2. Activate restoration functions as required.
3. Monitor Equipment Room restoration activities.
4. Maintain interface with vendors.
5. Coordinate as required (and directed) with other associated teams:
   a. Facilities
   b. Risk Management
   c. Transportation
   d. Purchasing
   e. Security
   f. Legal
6. Contact vendors; request an on-site representative, if required.
7. Document and log recovery efforts.
8. Evaluate salvageable status with Equipment Recovery Team Leader.
9. Coordinate move and storage of salvageable items to alternate facility.
10. Determine need to order equipment.
11. Monitor repair of damaged equipment.
12. Coordinate installation and testing of equipment.
13. Coordinate movement of personnel, equipment and material.

Who?

Selected technical services personnel.
Equipment Recovery Team (Affected Site).

What?

Organize salvage and recovery activities at the affected (damaged) site.

Why?

1. Direct damage assessment activities (repairs and replacement).
2. Activate restoration functions as required.

3. Monitor equipment room or equipment restoration activities.
4. Maintain interface with vendors.
5. Coordinate as required (and directed) with other associated teams:
   a. Facilities
   b. Risk Management
   c. Transportation
   d. Purchasing
   e. Security
   f. Legal
6. Determine extent of equipment damage.
7. Contact vendors; request an on-site representative.
8. Contact equipment restoration companies, such as BMS Catastrophe or ServPro.
9. Documentation and logging of recovery efforts.
10. Evaluate salvageable status.
11. Coordinate move and storage of salvageable items with Equipment Installation Team Leader.
12. Determine need to order equipment.
13. Monitor repair of damaged equipment.
14. Coordinate installation and testing of equipment.
15. Coordinate movement of personnel, equipment, and material.

Who?

Selected technical services personnel.

List Responsible Individuals' Names Here:

Department	*Primary/Alternate*	*Home Phone*	*Result of Alert*
Equipment Installation Team			

Notes:

_____

_____

Systems Software and Data Retrieval Team

What?

Coordinate retrieval of off-site stored materials.

Why?

A. Administrative Tasks

1. Participate in the Recovery Chief's activation meeting.
2. Maintain good written documentation of all changes and modifications to current operating procedures in anticipation of return to normal operations.
3. Maintain a record, with receipts when possible of all personal expenses incurred during the recovery operation.
4. Prepare a Network Systems Software Status Report and forward to the Central Support Coordinator.
5. Provide filenames and description to the off-site storage companies and request retrieval from the alternate site.
6. Verify that the data and items retrieved are correct.
7. Arrange to have documentation copied and one set returned to off-site storage.
8. Alert the software vendors, if necessary, using the Software Vendor Checklist in Appendix 8.
   a. Request any required vendor support.
   b. Ask vendor if the package will run on a different PBX or open system.
   c. If the software will not run on the newer hardware, request patches for the new environment or new software.
9. Reload all required disk data using available backups. Verify that data is properly loaded.
10. Bring up and test the network systems software.
11. Contact the Affected Site Team Leader and the Central Support Coordinator and provide an estimate of when systems and software configuration will be ready for recovery operations.
12. Assist with problem resolution and installation of resolutions or fixes.

Who?

Selected technical services personnel or transportation team members.

Responsible Individuals List Their Names Here

Department	*Primary/Alternate*	*Home Phone*	*Result of Alert*
System Software/Date Retrieval Team			

Notes:

Related Support Teams

The following are related disaster recovery functions that may be already in place, most likely in the existing Corporate Plan. Because close coordination will be required between MIS, Telecommunications, and Facilities departments for a total recovery effort, it is advisable to understand their functions. It also avoids duplication of effort, by allowing one off-site storage team, for example, to serve several different departments.

Human Resources Team

Team 1

Support Activities:

1. Provide a representative at Recovery Headquarters.
2. Notify families of injured personnel; explain benefits program.
3. Medical insurance coverage:
   a. Wage continuation.
   b. Employment continuation.
   c. Special considerations.
   d. Obtain temporary personnel during the recovery operation.
4. Arrange for senior management to present briefings to the personnel affected by the disaster. The purpose of the briefing is to address the organization's ability to successfully recover from the disaster and ensure employees of their job continuance.
5. Give special considerations to employees who were required to work during recovery compared to who were required to stay home.
6. Provide guidance on pay and compensation for employees.
7. Be prepared to provide list of employee home addresses if needed during the recovery operation.

Department	*Primary/Alternate*	*Home Phone*	*Result of Alert*
Human Resources			

Facilities Team

Team 2

Support Activities:

1. Provide a representative at Recovery Headquarters.
2. Provide guidance to local authorities accessing the facility, who will be unaware of the existence of unique preventative measures (lexon windows, automatic locking doors, raised floors, etc.)
3. Provide assessment of investigation of the cause.
4. Assist in the assessment of building damage:
   a. Architectural
   b. Electrical
   c. Utilities
   d. Environment (HVAC)
5. Manage building repairs and reconstruction activities.
6. Manage disposal of damage residue.
7. Obtain temporary Recovery Headquarters location.
8. Obtain temporary work locations.

Department	*Primary/Alternate*	*Home Phone*	*Result of Alert*
Facilities			

Finance Team

Team 3

Support Activities:

1. Provide a representative at Recovery Headquarters.
2. Alert appropriate corporate and company financial departments.
3. Provide immediate emergency credit arrangements, petty cash, and travel advances:
   a. Air travel and lodging
   b. Gasoline
   c. Ground transportation (rental car, taxi, etc.)
   d. Parking
   e. Tolls
   f. Food
   g. Miscellaneous out-of-pocket expenses
4. Provide communications with Tax regulatory agencies (federal, state, and local).
5. Assist in the investigation to account for any "lost" or destroyed negotiable items.

Department	*Primary/Alternate*	*Home Phone*	*Result of Alert*
Finance			

Risk Management Team

Team 4

Support Activities:

1. Provide a representative at Recovery Headquarters.
2. Notify the appropriate insurance companies:
   a. Obtain written releases.
   b. Obtain "Proof of Loss" documentation instructions (photographs).
   c. Obtain claims filing instructions.
3. Provide guidance regarding actions to be taken during the salvage operations:
   a. Provide necessary support documentation.
   b. Complete all "Proof of Loss" forms.
   c. Process all insurance claims.
4. Advise recovery personnel as to the type of records and information to be retained for insurance purposes:
   a. Provide special General Ledger account number to record recovery cost only.
   b. Collect and record all recovery-related costs.
5. Provide special insurance coverage:
   a. Temporary operations location.
   b. Personal auto riders for personnel who use their own vehicles during recovery.
   c. Revise Fleet insurance to allow messenger vehicles to transport personnel during recovery.
6. Coordinate with the Employee Relations representative to provide the proper handling of workers' compensation claims.
7. Provide insurance recovery for future loss charge created as a result of malfunctions experienced on equipment repaired as initially directed by the insurance company.

Department	*Primary/Alternate*	*Home Phone*	*Result of Alert*
Risk Management			

Internal Audit Team

Team 5

Support Activities:

1. Provide a representative at Recovery Headquarters.
2. Assist Security as required to coordinate investigations during the recovery.
3. Monitor computer processing of applications if processing must be performed with "out-of-balance conditions."
4. Verify that controls are in place for applications modified to meet limited resources available at the computer backup site.
5. Verify that controls are in place on data generated from computer processing of a critical application and needed for input to an unscheduled application.
6. Review recovery procedures to ensure assets control.
7. Notify external auditors, if necessary.

Department	*Primary/Alternate*	*Home Phone*	*Result of Alert*
Internal Audit			

Labor Relations Team

Team 6

Support Activities:

1. Provide a representative at Recovery Headquarters.

Department	*Primary/Alternate*	*Home Phone*	*Result of Alert*
Labor Relations			

Legal and Regulatory Team

Team 7

Support Activities:

1. Provide a representative at Recovery Headquarters.
2. Handle legal issues with "next of kin."
3. Advise recovery personnel on contractual obligations.
4. Existing equipment contracts.
5. New equipment contracts.
6. Real estate contracts.
7. Customer commitment contracts.
8. Provide copies of contracts destroyed by the disaster.

Department	*Primary/Alternate*	*Home Phone*	*Result of Alert*
Legal			

Medical Services Team

Team 8

Support Activities:

1. Provide a representative at Recovery Headquarters.
2. Handle minor medical requests.
3. Coordinate with local hospitals for additional medical requirements.
4. Identify and locate injured personnel already moved to the hospital.
5. Assist in obtaining proper food for recovery personnel during initial stages of the recovery operation.
6. To avoid exhaustion, ensure that recovery team members work reasonable hours.

Department	*Primary/Alternate*	*Home Phone*	*Result of Alert*
Medical			

Security Team

Team 9

Security Support Activities:

1. Provide a representative at Recovery Headquarters.
2. Provide security at all recovery operation locations.
3. Coordinate with the Corporate Security officers to provide:
   a. Control of investigations for the cause of the disaster.
   b. Liaison with local law enforcement and fire prevention agencies.
   c. Notifications to OSHA of the disaster situation.
   d. Coordinate with Risk Management representatives to get approval for the removal of any material from the damaged site.

Department	*Primary/Alternate*	*Home Phone*	*Result of Alert*
Security			

Mail Services Team

Team 10

Mail Services Support Activities:

1. Provide a representative at Recovery Headquarters.
2. Alert Post Office to advise of the situation.
3. Establish a Mail Services area within Recovery Headquarters to handle mail for recovery personnel.

Shipping & Receiving Support Activities:

1. Provide a representative at Recovery Headquarters.
2. Establish area to accept deliveries 24 hours a day.
3. Verify and maintain all paperwork related to receipts.
4. Develop control for further movement of all materials.
5. Maintain record of all special charges.

Department	*Primary/Alternate*	*Home Phone*	*Result of Alert*
Mail Services			

Public Affairs Team

Team 11

Support Activities:

1. Provide a representative at Recovery Headquarters.
2. Coordinate radio and TV announcements to notify employees as to where they will report.
3. Prepare official company statement to minimize adverse publicity.
4. Direct and coordinate all press conferences.
5. Provide, monitor, and control photographer.
6. Develop recovery progress notifications for publication:
   a. Internal newsletters.
   b. Stockholders' newsletters.
   c. Outside news media.

Department	*Primary/Alternate*	*Home Phone*	*Result of Alert*
Public Affairs			

Purchasing Team

Team 12

Support Activities:

1. Provide a representative at Recovery Headquarters.
2. Obtain office equipment, furniture, forms, and supplies, as needed:
   a. To replace unsalvageable items.
   b. For the alternate operating sites.
3. Issue purchase orders for all recovery requisitions.
4. Obtain an emergency replacement of computer forms needed for immediate processing during the recovery operation.
5. Identify and record special delivery or temporary storage costs.

Department	*Primary/Alternate*	*Home Phone*	*Result of Alert*
Purchasing			

Transportation Team

Team 13

Support Activities:

1. Provide a representative at Recovery Headquarters.
2. Provide ground transportation (trucks, station wagons, etc.):
   a. Retrieve backup files, documentation, forms, and supplies.
   b. Move salvageable equipment and materials.
   c. Transport supplies to alternate operations sites.
   d. Transport personnel.
3. Provide courier coordination and scheduling.
4. Provide air transportation:
   a. Company plane.
   b. Commercial plane.
   c. Private plane.
5. Obtain hotel accommodations.

Department	*Primary/Alternate*	*Home Phone*	*Result of Alert*
Transportation			

OTHER USEFUL FORMS AND CHECKLISTS

Facility Status Form for Report to EMT

Use this form to record the status of damage to the facility. Upon completion of the evaluation, prepare a Physical Damage Assessment Status Report and submit to the Affected Site Team Leader.

System	*Status*
Utilities/Services	
Electrical	
Lighting	
Heating	
Power cooling equipment	
Telephones	
Communications	
Plumbing	
Water supply	
Fire protection	
Security system	
Elevators	
UPS system (batteries and equipment)	
Motor generator area	
Motor generator backup	
Power	
Computer	
Source equipment	
Separate transformer	
UPS	
Engine generator	
Miscellaneous Power Considerations	
Power regulation	
Power distribution	
Computer system motor generator wiring	
Circuit breakers and power cables/cord	

Power Failure Phones

Most phones in large enterprises using PBXs will not work in a major disaster. Identify Power Failure Phones here.

Power Failure Phone Numbers

Original Number	*Location/Plant*	*Power Failure Number*

Equipment Inventory Form

Most of the equipment inventory for _____ Telecommunications is automatically updated. In the event a long-hand form is required, please use this one.

Equipment:

_____

Manufacturer:

_____

Serial number:

_____

Purpose:

_____

Criticality rating (1, 2, 3, 4):

_____

Date of purchase:

_____

Remarks:

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Software Inventory Form

Most of the software inventory for _____ Telecommunications is automatically updated. In the event a long-hand form is required, please use this one.

Equipment:

_____

Manufacturer:

_____

Serial number:

_____

Purpose:

_____

Criticality rating (1, 2, 3, 4):

_____

Date of purchase:

_____

Remarks:

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Priority Telephones for Recovery

A plan should include arrangements to restore critical phones, but larger locations may have to prioritize. List your most critical numbers here for priority in recovery. Remember, FAX lines count as phones.

Telephone Number	*Location*	*Purpose/Owner*

Plan Distribution Forms

A complete copy of the _____ Corporate Disaster Recovery Plan or parts thereof will be distributed to the following individuals:

The following individuals have received complete copies of the plan:

Copy#	*Name*	*Sections*	*Date Received*	*Date Returned*

Plan Distribution Form

The following individuals have received partial copies of the plan, such as the Table of Contents, Introduction, Maintenance & Distribution, appendices, and other sections (with associated checklists) indicated below:

Copy#	*Name*	*Sections*	*Date Received*	*Date Returned*

Acknowledgment of Receipt Form

To:
Subject:

The _____ Corporation Information Technology Disaster Recovery plan is distributed to authorized personnel to assist them in the understanding and performance of responsibilities and procedures related to the activation of their Disaster Recovery procedures.

The plan is intended for the individual's use while an employee of_____ _____ Corporation. Upon any departmental or company change of employment status, it is the responsibility of the individuals to return their assigned copy or sections of the Disaster Recovery Plan to the Data Control Manager, and fill out the change form contained in Appendix 3.

The recipient, in turn, will be responsible for the proper maintenance and security of the plan for as long as it is so assigned. The holders of the plan or any parts thereof will not allow unauthorized copying, review, or audit of the manual. No one outside of _____ Corporation will be permitted to read, review, or audit the plan without prior written approval from the Director, Information Technology. Individual copies of the plan or sections will be subject to review and audit at the request of the Director, Information Technology.

The undersigned does therefore acknowledge the receipt of the subject plan or sections and does understand and concur with the maintenance and security conditions above.

Receipt acknowledged by: _____

Director, Information Technology: _____

Date: _____

For the position of:_____

Date of receipt: _____

Return acknowledged by:_____

Date of return: _____

Information Technology Department Personnel Notification Information

This data-gathering form is used to create the IS department personnel notification checklist. This checklist will be used to notify employees of the activation of the plan and to advise them as to what they are supposed to do.

Fill out the information for each team leader, alternate team leader, required team member, or alternate member.

Employee name:_____

Job title: _____

Department name:_____

Home phone: _____

Cell phone: _____

Beeper: _____

Address (street): _____

Address (city, state, zip code):_____

Recovery team: _____

Location: _____

_____

Replacement (if applicable)

Employee name:_____

Job title: _____

Department name:_____

Home phone: _____

Cell phone: _____

Beeper: _____

Address (street): _____

Address (city, state, zip code):_____

Recovery team: _____

Location: _____

Termination Checklist

_____Corporation Corporate Headquarters
Name _____ Social Security No._____
Date of Termination _____ Last Day Worked _____

Company Credit Cards & Key	**Initials**
Air travel card	_____
Car rental card	_____
Telephone card	_____
Company equipment	_____
Building cardkey/keys	_____
American Express card	_____

Disaster Recovery

Disaster Recovery Team member? Yes_____ No_____

If yes, which department and team?

_____

Health Care Cards	**Initials**
Paid	_____

Corporate Expense Account

Amount due to the company $ _____

Amount due to the employee $ _____

Cleared? _____Yes _____ No

Benefits/Conversion Forms	**Initials**
LTD (Disability Conversion Insurance)	_____
Savings & Investment Plan	_____
Voluntary Group Accident Insurance	_____
Noncontributory Life Insurance	_____
COBRA Notification	_____
Deferred Vested Pension Calculation	_____
Retirement Eligible Pension Calculation	_____
Group Universal Life Insurance	_____
Termination Form	_____

Forwarding Address
Address/P.O. Box _____City, State, Zip _____
Area Code/Telephone No. _____ _____
(Report Address Changes to the _____ Human Resources Department)
_____ _____

Authorization
Employee acknowledgment _____ Date _____
Supervisor or department head _____Date _____
Human Resources manager _____Date _____

Notes:

Special Equipment/Disaster Agreements

List here:

Hardware Lists and Serial Numbers

List the following here:

Equipment	*Function*	*Serial Number*

Software Lists and License Numbers

List the following here:

Software	*Function*	*License Number*

Vendor Call-Out and Escalation List

List the following here:

Vendor Number	*Manager*	*Number*

Carrier Call-Out and Escalation Lists

List the following here:

Carrier Number	*Escalation Number*

Network Schematic Diagrams

Equipment Room Floor Grid Diagrams

Employee Inventory

List the following here:

Employee	*Title Function*	*Home Phone*	*Wireless Phone*

Reference to Contract and Maintenance Agreements

Equipment	*Notes*

Use additional pages as necessary.

References to Operating Instructions for Equipment

Special Notes on Equipment	

Use additional pages as necessary.

Crisis Management

Consider identifying a formal Crisis Management Team.

The Crisis Response Team (aka EMT)

A Crisis Response Team is hereby established at _____ Corporate Headquarters, which shall consist of the following members and alternates:

Function	*Member*	*Alternate*
Executive in Charge	President and Chief Executive Officer	General Counsel
Financial	Vice President, Controller, and Treasurer	Assistant Treasurer
Legal	Vice President, Secretary, and General Counsel	Associate General Counsel
Employee Relations	Vice President, Employee and Community Relations	Compensation
Security	Director, Government Compliance	
Public Affairs Media Contac	Director, Investor Relations	

The names, office, and residence telephone numbers of the current members of the Crisis Response Team and their alternates as of the origination date of this CMP are set forth in the Schedule. This Schedule will be updated as changes occur.

The Crisis Response Team shall determine and manage _____'s handling of news-media-sensitive situations, providing direction, guidance, and assistance to the local business unit involved. The Crisis Response Team shall also be responsible for the handling or supervision of responses to press and other media inquiries concerning news-media-sensitive situations and disaster situations.

Now You Are on Your Way

Appendix 2

Partial Glossary of Telecommunications Terms and Acronyms

Leo A. Wrobel

Over the years we have often heard people complain that telecommunications is the most acronym-ridden occupation in the galaxy or at least in the immediate solar system. This may in fact be true. The trouble is nobody really knows all the acronyms unless they work in the telecom business and even then new ones pop up constantly.

In an effort to help assuage this problem we have provided a handy reference here for you in the form of a modest telecommunications glossary. When you are working with your telephone company on how you can add resiliency to your wide-area network (that's also WAN, look it up below) these definitions just might be the ticket to better communication. With that said, here goes:

Acronym	Description
A&A	Annoying & Anonymous Bureau (see ACB)
A/D	Analog to Digital conversion
A/T	Access/Tandem
AAB	Automatic Answer Back
AABS	Automated Alternate Billing Service; Automated Alternate Billing System (system where O+ calls are billed)
AAP	Alternate Access Provider
ABS	Alternate Billed Screening (DBAC); Alternate Billing Service
AC	Access Customer; Alternate Community (in PREMIS); Automatic Call (Back)
ACAT	Additional Cooperative Acceptance Testing
ACB	Annoyance Call Bureau; Automatic Call Back
ACC	Access Information
ACD	Automatic Call Distributor system
ACES	Automatic Control Encryption System (E9-1-1)
ACH	Automated Clearinghouse
ACN	Access Carrier Name; Advanced Communication Network; Access Customer Name
ACNA	Access Carrier Name Abbreviation (Bellcore—assigned)
ACQS	Access to Charge Quotation System (SWBT)
ACR	Anonymous Call Rejection
ACRJ	Automatic Caller Rejection
ACS	Annoyance Call Specialist
ACT	ASR Activity Type
ACTEL	Access Telephone Number
ACTL	Access Customer Terminal Location
AD	Application Date; Assignment Date
ADA	Application Data Access (Service Manager term)
ADDR	Address
ADL	Additional Directory Listing
ADN	Advanced Digital Network
ADVC	Advanced/Payment/Deposit Verification
AECN	Alternate Exchange Carrier Number (SWBT term synonymous with an OCN)

AF	Alternate Final (overflow trunk in E9-1-1 Service)
AFR	Automatic Flexible Routing
AGAUTH	Agency Authorization Status
AGG	Aggregation
AI	Address Info
AIN	Advanced Intelligent Network; Advanced Intelligence Network
AIN-SCP	Advanced Intelligence Network - Service Control Point
AIOD/IOD	Automatically Identified Outward Dialing/Identified Outward Dialing
AIS	Airport Intercommunicating Service (Centrex); Automatic Intercept Service
ALB	Additional Labor Billing
ALI	Automatic Location Identification; Automatic Location Identification System (E911 service)
ALIS	Automatic Location Identification System
ALRU	Automatic Line Record Update (in LMOS)
ALT	Automatic Line Testing
ALTTSC	Alternate Two Six Code
AMA	Automated Message Accounting; Automatic Message Accounting (recordings); Automated Message Announcements
AML	Additional Main Listing
ANC	All Number Calling
ANE	Assembly of Network Elements (UNE)
ANI	Automatic Number Identification
ANSI	American National Standards Institute
AO	As Of (date)
AOCN	Administrative Operating Company Number
AP	Access Provider; Accounts Payable; Adjustments Applied; Advance Payment
AP/DV	Advanced Payment/Deposit Verification
APOT	Additional Point Of Termination
APP	Application Date
APPT	Appointment
APSAG	Access Provider Street Address Guide
APTOS	Automatic Pricing

ARS	Automatic Route Selection
ARSB	Automated Repair Service Bureau
ASCII	American Standard Code for Information Exchange
ASOG	Access Service Ordering Guidelines (SWBT)
ASR	Access Service Request
ASR-NO	Access Service Request Number
ASYNC	Asynchronous
AT	Access Tandem
ATAB	Area Trunk Assignment Bureau
ATAB/TAG	Area Trunk Assignment Bureau/Translation Assignment Group
ATC	Access Tandem Code
ATH	Abbreviated Trouble History
ATIS	Alliance for Telecommunications Industry Solutions
ATM	Asynchronous Transfer Mode
ATN	Access Tandem Network; Account Telephone Number, Associated Telephone Number
ATS	Advanced Telecommunications Services
AUL	Alternate User Listing
AUR	Access Usage Record
AUTH	Authorization code
AVRU	Automated Voice Response Unit
AWC	Area Wide Centrex
BACR	Billing Account Cross Reference
BAG	Billing Account (Aggregation) Group
BAID	Billing Account ID
BAL	Business Answering Line
BAN	Billing Account Number
BAR	Billing Account Reference
BAUD	A unit of signaling speed (one baud corresponds to a rate of one signal element per second)
BBG	Business Buyer's Guide
BBS	Bulletin Board System
BCC	Bellcore Client Company

BD	Balance Due; Bill Date
BDN	Billing Directory Number
BDT	Billing Data Tape
BER	Bit Error Rate
BES	Basic Exchange Services
BF	Bill Face
BFR	Bona Fide Request (SWBT)
BHMC	Busy Hour Minutes of Capacity
BHMS	Busy Hour Minutes
BILL CON	Bill Contact name; Billing Contact name
BILL NM	Billing Name
BILLNUM	Bill Number
BL	Basic Link
BLK	Block 900/976 Calls
BLV	Busy Line Verification Code (trunk groups)
BLV/BLI	Busy Line Verify/Busy Line Interrupt
BLVI	Busy Line Verification & Intercept
BM	Bill Message
BN	Billing Number
BNA	Bill Name and Address
BNS	Billed Number Screening
BOC	Bell Operating Company
BOC-CATS	National Bell Operating Company Credit Card and Third Number System (SWBT)
BOC ID	Bell Operating Company (circuit) Identification
BOCP	Billing Optional Calling Plans or Plus; Business Optional Calling Plan
BP	Binding Post
BR	Bill Round
BRA	Basic Rate Area (ISDN)
BRADS	Bellcore Rating Administrative Data System(s)
BRDE	Billing Records Data Exchange
BRI	Basic Rate Interface
BRIDS	Bellcore Rating Input Database System

BRUD Business Resale Usage Discount

BTN Billing Telephone Number

Bellcore Bell Communications Research

CABS Carrier Access Billing System

CADS Computer Aided Dispatch System (E9-1-1)

CAMA Centralized Automatic Message Accounting

CAPS Carrier Access Providers; Competitive Access Providers

CAR Current Activity Report (see CUR)

CARE Customer Account Record Exchange

CATS Credit Card and Third-Party System

CBCAD Cannot Be Completed As Dialed

CBT Computer-Based Training

CCC Cellular Call Completion; Customer Care Center

CCCC Customer Controlled Cross Connect

CCCS Centralized Credit Check System

CCECC Co-Carrier Equipment Cross Connect (also called cage to cage)

CCL Carrier Common Line

CCLC Carrier Common Line Charge

CCN Certificate of Convenience and Necessity (SWBT)

CCNA Customer Carrier Name Abbreviation

CCON Customer Contact

CCRS Centrex Customer Rearrangement System

CCS Calling Card Service; Cellular Call Completion; CESAR Customer Support; Common Channel Signaling; Customer Calling Services

CCS7 Common Channel Signaling System 7

CCSA Common Channel Signaling Access capability (provides SS7 signaling for FG-D)

CCSN Customer Contact Service Name; Customer Contact Service Node

CCSNIS Common Channel Signaling Network Interface Specifications

CCV Calling Card Validation

CCW Cancel Call Waiting

CD Circuit Details; Completion Date

CD/SENT Confirmation Date and time Sent
CDA Customer Directory Assistance
CDAR Customer Dialed Account Recording
CDC Customer Data Change
CDDD Customer Desired Due Date
CDLR Confirming Design Layout Report
CDLRD Confirming Design Layout Report Date
CEF Cooperative Entrance Facility
CENTREX Central Office Exchange Service
CESAR Customer Enhanced System for Access Requests
CEV Controlled Environment Vaults
CFA Channel Facility Assignment; Connecting Facility Assignment
CFAU Connecting Facility Assignment Use
CFB Call Forwarding Busy
CFBL Call Forwarding Busy Line
CFNI Carrier's Fiber Network Identification
CFW Call Forwarding
CH Clearinghouse
CI Carrier Interconnection; Confidential Information; Credit Information
CIC Carrier Identification Code
CIDB Circuit Information Database
CIR Committed Information Rate
CKID Circuit Identification
CKL Circuit Location
CKLT Circuit Location; (Central office interface point bridging location) Termination
CKR Circuit Identification (CLEC assigned)
CKTID Circuit Identification Number
CKT Circuits
CLASS Customer Local Area Signaling Services; Customer Local Area Switching Services
CLC Carrier Liaison Committee; Common Language Code
CLCI Common Language Code Identifier

CLCICL Competitive Local Carrier Interconnection Network Element Commitment Letter (INER term)

CLEC Competitive Local Exchange Carrier

CLECA Competitive Local Exchange Carrier A (used to describe calls between 2 CLECs)

CLECB Competitive Local Exchange Carrier B (used to describe calls between 2 CLECs)

CLF Common Language Facility

CLFI Common Language Facility Identification

CLH Classified Listing Header

CLI Calling Line Identification

CLID Calling Line ID Display

CLLI Common Language Location Identification

CLS Circuit Identification (P*B assigned)

CLSV Class of Service

CMDB Centralized Message Database

CMDS Centralized Message Data System; Centralized Message Distribution Service; Centralized Message Distribution System

CMRS Commercial Mobile Radio Service

CMS Centrex Management Service

CNA Customer Network Administration (SWBT)

CNAM Caller ID Name; Calling Name Delivery (SWBT)

CNB Call Number Blocking

CND Calling Directory Number Delivery; Calling Number Delivery

CNDB Calling Number Delivery Blocking

CNDS Calling Name Delivery Service

CNI Common Network Interface

CNL Customer Name and Location Bureau

CNNB Calling Number Blocking

CNR Customer Not Ready

CNSC Customer Network Service Center

CO Central Office

COC Central Office Code

COCAG Central Office Code Assignment Guidelines

COCARC Central Office Code Assignment Request & Confirmation

COCOT Customer-Owned Customer-Operated Telephone (pay phone)

COMM Community Code

COPT Customer-Owned Pay Telephone (now called PSP [Payphone Service Provider])

COPW Customer-Owned Premises Wire

COT Customer-Originated Trace (SWBT)

CPAC Circuit Provisioning Assignment Center

CPAT Competitive Provider Account Team

CPCN Certificate of Public Convenience and Necessity; Certified Public Company Number

CPE Customer Premises Equipment; Customer Provided Equipment

CPG Call Pickup Group

CPIW Customer Provided Inside Wire

CPM Cost Per Minute

CPN Calling Party Number: Customer Proprietary Number

CPNI Customer Proprietary Network Information

CPP/PPP Calling Party Pays/Paging Party Pays (wireless term)

CPR Call Processing Records

CPU Call Pick Up

CPUC California Public Utilities Commission

CR Call Return

CRDD Customer Requested Due Date

CRIS Customer Record Information System

CRMN Customer Return Migration Notification

CRMS Central Reliable Message Service

CRO Completed Related Order (a FID)

CRS California Relay Service (for the deaf): Cell Relay Service

CS Call Screen: Class of Service

CSB Customer Service Bureau; Customer Service Bureau (611)

CSFT Customer Services Features Translator

CSN Call Screening; Customer Service Node

CSR Customer Service Record

CST Cooperative Scheduled Testing

CSU/DSU	Channel Service Units/Data Service Units
CT	Call Trace; Channel Termination; Common Transport
CTC	Call Trace Center
CTO	Cut Through
CTX	CENTREX
CUD	Casual User Dialing
CUR/CAR	Code Use Record/Code Activity Record
CUS	Customer Code
CVN	Customer Virtual Network
CWG	Call Waiting
CWI	Call Waiting Indicator
CWL	Call Waiting Lamp; Circuit Work Location
CXR	Call Transfer
D/TREC	Date and Time Received
D/TS	Date and Time Sent
DA	Digital Access; Directory Advertising; Directory Assistance
DAA	Directory Assistance (only) Additional listing
DAC	Directory Assistance Charge
DACC	Directory Assistance Call Completion
DACS	Digital Access Connect System
DAE	Directory Assistance (charge) Exemption (for deaf & disabled)
DAL	Dedicated Access Line; Directory Assistance Listing (listings only in Directory Assistance database)
DAM	Directory Assistance only Main listing
DAO	Directory Assistance Only listing
DBAC	Data Base/Database Administration Center (validates billing services such as calling card PINS and Billed Number Screening [BNS])
DBMS	Database Management System
DC	Direct Connection
DCC	Data Communication(s) Channel
DCCS	Digital Cross-Connect System
DCF	Delay Call Forwarding
DCP	Data Control Point

DCS Digital Cross-Connect System; Digital Cross Connect
DD Due Date
DDD Desired Due Date; Direct Distance Dialing
DDI Direct Digital Interface service (Centrex)
DDN Dialable Directory Number
DDOV Digital Data Over Voice service
DDS Deaf & Disabled Service; Digital Data Service
DE Data Exchange
DEF Digital Entrance Facilities
DEP Deposit (a FID)
DFI Digital Facility Interface
DID Direct Inward Dial
DIDR Direct Inward Dial Number Range
DIF Digital Interface Frame
DIU Data Integrity Units (E9-1-1)
DL Dial Line
DLA Directory Listing Assignment
DLC Digital Loop Carrier
DLH Distributed Line Hunting
DLN Digital Line Number
DLR Design Layout Reports; Directory Listing Requirement; Display Line Record (LMOS)
DLRD Design Layout Report Date
DLTU Digital Line and Trunk Unit
DMLR Display Mini Line Record (LMOS)
DMS Data Management (E9-1-1); Digital Multiplex System (Central Office)
DN Directory Number
DNA Data Network Address
DNAL Dedicated Network Access Link
DNC Digital Network Controller
DNCF Directory Number Call Forwarding
DND Do Not Disturb
DNH Directory Number Hunting

DNIC	Data Network Identification Code
DNIS	Dialed Number Identification Service
DNR	Do Not Refer
DNRI	Directory Number Route Index
DOD	Direct Outward Dial
DP	Dial Plus
DPA	Different Premises Address
DPR	Dispute Resolution Procedure
DPRG	Directory Purge
DQDT	Delete Quick Dial Tone
DR	Distinctive Ringing
DRCW	Distinctive Ringing/Call Waiting
DRING	Distinctive Ring
DS	Data Services; Digital Multiplexing; Directory Services
DS-0	Digital Signal Level 0
DS-1	Digital Signal Level 1
DS0	Digital Signal Level 0
DS1	Digital Signal Level 1
DS3	Digital Signal Level 3
DSCR	Directory Service Caption Request (SWBT)
DSCT	Disconnect (FID)
DSGCON	Design Contact; Design/Engineering Contact
DSL	Digital Signal Level
DSR	FID that places a listing in both residence and business
DSU/CSU	Data Service Unit/Channel Service Unit (Customer interface for DDS channel bank)
DSX	Digital Cross Connect
DT	Dedicated Transport; Dial Tone
DTF	Dial Tone First (coin telephones)
DTMF	Dual Tone Multifrequency signaling (touchtone)
DTN	Dial Telephone Number
DTR	Detailed Trunk Record
DTT	Direct Trunked Transport
DV	Directory Validation

DX	Duplex Signaling
E&M	Ear and Mouth (signaling)
E9-1-1	Emergency 911 database
EA	Equal Access
EABS	Exchange Alternate Billing Services
EAEO	Equal Access End Office
EAMF	Equal Access Multifrequency
EAOSS	Equal Access Operator Services Signaling
EAR	Easy Access Request (menu in CESAR)
EARS	Easy Access Request System
EARTG	End Office Alternate Traffic Routing
EAS	Equal Access Signaling; Extended Area Service; Extended Area Service
EASE01	Easy Assess Sales Environment
EAT	Equal Access Tandem
EB	Electronic Bonding
EBI	Electronic Bonding Interface
EBP	Extended Billing Plan
EBS	Electronic Business System (set)
EC	Exchange Carrier/Company
ECC	Emergency Control Center; Express Call Completion (DA)
ECCKT	Exchange Company Circuit ID
ECIC	Electronic Communication Implementation Committee
ECSPC	Exchange Carrier's Signaling Point Code (SONET)
EDAS	Engineering and Administration Data Acquisition System
EDI	Electronic Data Interchange; Electronic Data Interexchange
EDIB	Electronic Data Exchange/Interexchange Billing
EDLS	Electronic Directory Listing Service
EDSL	Extended Digital Subscriber Line
EDSX	Electronic Digital Signal Cross Connect
EF	Entrance Facility
EFT	Electronic Funds Transfer
EGI	Electronic Gateway Interface
EI	Electronic Interface

EISCC	Expanded Interconnection Service Cross Connects (collocation)
EKTS	Electronic Key Telephone Service
ELCS	Extended Local Calling Service
EM	Electronic Monitoring; Equipment Masterfile
EMF	Exchange Masterfile
EMI	Exchange Message Interface
EMR	Exchange Message Record
EMR/EMI	Expanded Message Record/Expanded Message Interface
EO	End Office/End Office switch
EO/CO	End Office/Central Office
EOAR	End Office Alternate Routing (FG D)
EOAT	End Office Access Tandem
EOC	End Office Code
ES	Easy Saver (a type of usage discount plan)
ESB	Emergency Service Bureau
ESBA	Enhanced Summary Billing Arrangement
ESCO	Emergency Service Central Office code (E9-1-1)
ESL	Essential Line Service
ESMR	Enhanced Specialized Mobile Radio
ESN	Emergency Services Numbers (E9-1-1); Electronic Switched Network
ESP	Enhanced Service Providers
ESPP	Essential Service Protection Plan (ESL)
ESS	Electronic Switching System
ESSSCC	Electronic Switching System Switching Control Center
ESZ	Emergency Service Zone (E9-1-1)
ETF/EBS	Electronic Telephone Features/Electronic Business Set
ETN	Electronic Tandem Network
ETR	Estimated Time of Restoral
ETS	Electronic Tandem Switching
ETTR	Estimated Time To Repair
EU	End User
EUCL	End User Common Line Charge

EUM	End User Migration
EUN	End User Name
EUSA	End User Special Access
EUTEL	End User Telephone Number
EX	Exchange (and Central Office)
EXCO	Exchange and Central Office Code
EXP	Expedite
EXT	Exit Message (SS7)
F&T	From and To (service location move)
F-LSC	Facilities Local Service Center
FABS	Flexible Automated Billing System
FACS	Facility Assignment and Control System
FACTL	Facility Access Customer Terminal Location
FANI	Flexible Automatic Number Identification (meet point billing)
FAX	Facsimile
FCC	Federal Communications Commission; Frame Control Center
FCKT	Facility Circuit Identification
FCMAC	Facility Maintenance and Administration Center
FDA	Foreign District Area
FDAS	Foreign District Area Service
FDD	Frame Due Date
FDF	Fiber Distribution Frame
FDI	Feeder Distribution Interface
FDLRD	Facility Design Layout Report Date
FDT	Frame Due Time
FEX	Foreign Exchange
FG	Feature Group
FG-A	Feature Group A—Line side connection from P*B
FG-B	Feature Group B—Trunk side connection from a P*B
FG-D	Feature Group D—Switched access product
FGA	Feature Group A
FI	Facility Interface
FID	Field Identifier
FLT	FID for 800 service additional listing—non-chargeable

FMAC	Facility Maintenance and Administration Center
FN	Fiber Node
FNA	USOC and FID for reference listing—different customer
FNI	Fiber Network Identification
FNPA/NN	Foreign Numbering Plan Area/New Number
FO	Fiber Optic; Firm Order
FOC	Firm Order Confirmation
FOT	Fiber Optic Terminal
FPOS	First Point Of Switching
FPP	Flexible Pricing Plan
FPS	Foreign Prefix Service
FR	Flat Rate
FRD	Flexible Route Design
FRL	Facility Restriction Level (Centrex ETS/ETN)
FRS	Flexible Rate Selection; Frame Relay Service
FRS/ARS	Flexible Route Selection/Automatic Route (features) Selection (Centrex)
FSO	Foreign Service Office
FTA	Federal Telecommunications Act
FTP	File Transfer Protocol
FWD TN	Forward to Telephone Number
FX	Foreign Exchange
FXS	Foreign Exchange Service
GAP	Generic Access Parameter (PNP Term)
GIR	Generic Interface Region
GPIC	Group Primary InterLATA Carrier (Centrex)
GR	Generic Requirements
GS	Ground Start
GSM	Global Standard Mobile; Global System for Mobile Communications
GST	Generic Switch Type
GSZ	Group Size
GTF	General Trunk Forecast
GUI	Graphical User Interface

HB	Hold Bill
HBAN	High Capacity Channel Billing Account Number
HC	High Capacity
HCDS	High Capacity Data Services
HCP	Handicapped Account
HDLC	High Level Data Link Control
HDSL	High-Bit Digital Subscribe Line; High Bit-Rate Digital Subscriber Line
HDW	Hardwired
HLR	Home Location Registry (wireless)
HML	FID for Multi-Line Hunt
HNPA	Home Numbering Plan Area
HNTYP	Hunting Type Code
HPF	Hunting Preferential List
HRO	USOC for Maintenance Visit Charge
HTC	FID for Circular Hunting
HTG	Hunting Serial
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
HTY	FID for Service Completion for Hunting
HUB	Multiple Bridging and Multiplexing Facility
HUNTG	USOC for Hunting—Business
HUNTR	USOC for Hunting—Residence
HVCI	High Volume Call-In Prefixes
HVLR	Home Visitor Local Registration (wireless)
HVP	High Voltage Protection
HWL	Hot/Warm Line
HiCAP	High Capacity Service
IACC	FID for Access Customer Address
IACN	Interexchange Access Carrier Name
IAD	Integrated Access Device
IAM	Initial Address Message (SS7)
IBC	Initial Billing Company
ICSC	Interexchange Carrier Service Center

ICSWE	Interexchange Carrier Serving Wire Center
ID	Identification; Issue Date
IDDD	International Direct Distance Dialing
IEC	Interexchange Carrier
IECDA	Interexchange Carrier Directory Assistance
IFWPL	Independent Foreign White Page Listing
IHML	FID for Multi-Line Hunt Group Number
IHTG	FID for Service Completion for Hunting
IJIP	Initial JANE Interconnection Point
ILCON	Local Contact Name
ILEC	Incumbent Local Exchange Carrier; Independent Local Exchange Carrier
ILIP	Initial LISA Interconnection Point
ILOC	FID required by LMOS for Location on Resale Order
ILP	IntraLATA Presubscription
IMPCON	Implementation Contact; Implementation Contact Name
IN	Intelligent Networks (AIN)
INA	Information Network Architecture; Integrated Network Address
INDCO	Independent Telephone Company
INE	Intelligent Network Element
INER	Interconnection Network Element Request
INETES	Intelligent Network Element Terminal Emulation System
INEXS	SWBT's transmittal system to send CARE records using TCSI codes
INP	Interim Number Portability
INPG	Industry Number Planning Guide
INTE	Intelligent Network Element
IO	Implementation Order
IOD	Identified Outward Dialing service (grandfathered)
IOF Node	Interoffice Facility Node
IOF Ring	Interoffice Facility Ring (SONET)
IOF	Interoffice Facilities
IOM	Interoffice Mileage

IOT	Interoffice Transport
IP	Information Provider; Internet Protocol
IRL	Individual Resale Line
IS	Integrated Services; Intercept Service
ISA	FID for Service Order on Resale order
ISCB	Information Services Call Blocking (900 and 976)
ISCP	Integrated Service Control Point (AIN)
ISDN	Integrated Services Digital Network ISDN Service Center
ISDNUP	Integrated Services Digital Network User Part
ISNI	Intermediate Signal Network Identifier
ISP	Information Service Provider; Internet Service Provider(s)
ISR	Interconnection Service Request
ISUP	ISDN User Part (SS7)
ITA	IntraLATA Trunk Group
ITC	Independent Telephone Companies
ITCO	Independent Telephone Company
ITDPL	International Telephone Directory Price List
ITE	InterLATA Trunk Group
ITNP	Interim Telecommunications Number Portability
ITR	Interconnection Trunking Requirements
IVD	Integrated Voice and Data
IVEN	Installation Vendor (collocation)
IVS	Interactive Voice System
IW	Inside Wire
IXC	Interexchange Carrier
IXCs	Interexchange Carriers
IXPL	Interexchange Private Line
JK CODE	Jack Code
JK NUM	Jack Number
JK POS	Jack Position
JUL	Joint User Listing
KP	Key Pulse
KTS	Key Telephone System
L-M	Land to Mobile (wireless)

LAB	Language Assistance Bureau
LAC	Loop Assignment Center
LADT	Local Area Data Transport
LAMA	Local Automatic Message Accounting
LAN	Local Area Network
LASR	Local Access Service Request
LASS	Local Area Signaling Services
LAT	FID that identifies LATA of ACTL
LATA	Local Access and Transport Area
LCA	Local Calling Area
LCC	Line Class Code
LCON	Local Contact
LD	Loop Distribution
LDC	Local Distribution Channel
LDI	Long Distance Indicator
LDN	Listed Directory Number
LDR	SWBT's Local Disconnect Report
LEA	Law Enforcement Agency
LEAS	LATA Equal Access System
LEC	Local Exchange Carrier
LED	Last Effective Date
LEGNUM	Multipoint Leg Number
LEN	Line Equipment Number
LERG	Local Exchange Routing Guide
LEX	LSR Exchange System
LFACS	Loop Facility Assignment & Control System
LHT	Last Hunting Termination
LIDB	Line Information Database
LISA	Local Interconnection Service Arrangement
LLAL	Local Loop Access Line (SONET)
LLAR	Local Loop Access Ring (SONET)
LLC	Line Load Control
LLLL	Line Number
LLT	(Additional) Listing Line

LM1 Land to Mobile Direction (wireless)
LM2-B Land to Mobile Blended (wireless)
LM2-U Land to Mobile Unblended (wireless)
LM3 Land to Mobile (calling party pays) (wireless)
LMOS Loop Maintenance Operations System
LNI Listed Number Indicator (yellow pages)
LNP Local Number Portability
LNR Last Number Redial
LOA Letter of Agency; Letter of Authorization (from end user)
LOC Local Operations Center
LP Late Payment; Loop
LP1 Land to Paging Direction (wireless)
LP2-B Land to Paging Blended (wireless)
LP2-U Land to Paging Unblended (wireless)
LPC Late Payment Charge
LPIC Local Primary Intra-LATA Carrier
LPS Loop Start
LRAF LSP Remote Access Facility (SWBT)
LRN Location Routing Number
LS Listing Services; Local Switching; Local Switching (LS1 &LS2); Loop Service (SWBT); Loop Start
LS1 Local Switching Rate (1 for FGA/B)
LSC Line Screening Code; Local Service Center; Local Switching Capability
LSDB Listing Services Database
LSINP Loop Service with Number Portability (SWBT)
LSNE Local Switching Network Element
LSNP Local Switching with Number Portability
LSO Local Serving Office
LSOG Local Service Ordering Guide (OBF National Standard)
LSOR Local Service Order Request
LSP Local Service Provider
LSPSC Local Service Provider Service Center
LSR Local Service Request

LT	LATA Tandem; Line Terminal; Local Transport; Loop Type
LTF	Local Transport Facility
LTL	Local Transport Location
LTP	Local Transport
LTR	Local Transport Rate Element; Local Transport Restructure
LTT	Local Transport Termination
LTU	Line Test Unit
LUD	Local Usage Detail
LVAS	Line Validation Administration System
LVAS	Line Validation Administration System (interfaces with LIDB) (SWBT)
LWT	LATA-Wide Terminating Indicator
LWTA	LATA-Wide Terminating Arrangement
M-L	Mobile to Land (wireless)
MA	Maintenance Administrator
MAC	Missed Appointment Code
MADN	Multiple Appearance Directory Number
MAPS	Mechanized Address Prevalidation System
MBA	Make Busy Arrangement
MBC	Multiple Bill Copies
MCU	Multiple Control Unit (group video)
MDF	Main Distribution Frame
MDR	Message Detail Recording
MDR-RAO	Message Detail Recording via Revenue Accounting Office
MDTGR	Message Design Trunk Group Record; Message Design Trunk Group Reply
MDU	Multiple Dwelling Unit
MDU/BCL	Multiple Dwelling Unit/Business Customer Location
MECAB	Multiple Exchange Carrier Access Billing; Multiple Exchange Carrier Access & Billing
MECOD	Multiple Exchange Carrier Ordering and Design
MF	Multi-Frequency
MI	Minimal Input (filter system in SORD); Machine Interface Code

MII	Minimal Input Inquiry (SORD)
MIIC	Minimal Input Inquiry Complex (SORD)
MIIS	Minimal Input Inquiry Simple (SORD)
MIR	Minimal Input Record/Request for Access
MITN	Move-In Telephone Number
ML1	Mobile to Land (wireless)
ML2	Mobile to Land Blended (wireless)
MLAC	Mechanized Loop Assignment Center
MLH	Multi-Line Hunt
MLHG	Multi-Line Hunt Group
MLR	Multi-Line Record
MLT	Mechanized Loop Testing (PBSM)
MM	Multiple Bill
MMC	Minimum Monthly Charge
MMUC	Minimum Monthly Usage Charge
MN	Miscellaneous Number
MNL	Main Listing
MOS	Modified Operator Services
MOSS	Modified Operator Services Signaling
MOTN	Move Out Telephone Number
MOU	Minutes Of Use
MPB	Meet-Point Billing
MPOE	Minimum Point Of Entry
MPOP	Minimum Point Of Penetration (wire)
MPT	Multiport Transreceiver
MR	Maintenance Request; Message Rate (ready)
MRC	Missed Reason Code; Monthly Recurring Charge
MRVT	MTP Routing Verification Test
MS	(E911) Management System; Minimum Service Charge
MSA	Metropolitan Statistical Area
MSAG	Master Street Address Guide
MSB	Mechanized Summary Billing
MSC	Maintenance of Service Charge; Mobile Switching Center
MSFI	Mid-Span Fiber Interconnection

MSL Multipoint Service Leg
MSN Mobile Serial Number (wireless)
MTA Metropolitan Trading Area
MTC Metallic Circuit
MTCE Maintenance Contact
MTL Minimum Termination Liability (SONET)
MTO Message Trunk Order
MTP Message Trunk Part
MTS Message Telecommunications Service; Message Telephone Service; Message Toll Service
MTSO Mobile Telephone Switching Office
MTU Magnetic Tape Unit; Maintenance Test Unit; Message Toll Unit
MU Message Unit
MUX Multiplex
MUXLOC Multiplexing Location
NAB USOC for Reference Listing (same customer)
NAC Network Administration Center; Number Assignment Center
NANP North American Numbering Plan
NB Nevada Bell
NC FID for No Charge; Network Channel; Network Channel Code; Network Code; New Connect
NC1 Network Channel Code (T1)
NCC Network Channel Code; Network Control Center
NCEO Non-Confirming End Office
NCI Network Channel Interface; Network Channel Interface code
NCK USOC for Change Telephone Number Charge
NDM Network Data Mover
NE Network Element; Network Engineering
NEBS Network Equipment Building System
NEC National Electrical Code
NECA National Exchange Carrier Association
NECA 4 National Exchange Carrier Association
NENA National Emergency Number Association

NFDD	New (switched access) Facility Due Date
NFDLRD	New (switched access) Facility Design Layout Report Date
NFI	New (switched access interface) Facility Identification
NFID	Non-fielded section of a SORD order
NFPA	National Fire Protection Association
NFQTY	New (switched access) Facility Quantity
NFWK	No Field Work
NHN	Non-Hunting Number
NHNI	Non-Hunting Number Indicator
NI	Network Interconnection; Network Interface
NIC	Network Interface Charge
NID	Network Interface Device
NIM	Network Interconnection Methods
NIU	Network Interface Unit
NMB	No Minimum Billing
NMSC	Network Management Service Center
NNI	Network to Network Interface
NNX	3-Digit prefix of a telephone number
NOB	Number Of Bills
NON-ZUM	Non-Zone Usage Measurement
NOP	Network Operations Protocol
NOR	Number Of Requests (ASRs)
NP	Non-Published number
NP3	USOC for Non-Published listing (non-chargeable)
NPA	Numbering Plan Areas; Numbering Plan Area (area code)
NPA/CUR	Numbering Plan Area/Code Use Record
NPA/NXX	Numbering Plan Area/Prefix
NPAC	Number Portability Administration Center
NPD	Non-Payment Disconnect; Numbering Plan Digit (E9-1-1)
NPS	Number Portability Service
NPU	USOC for Non-Published listing—chargeable
NRAO	Northern Region Revenue Accounting
NRC	Non-Recurring Charge

NRS	Network Reconfiguration Service (SWBT); Number Referral Service; Number Retention Service
NS	Non-Published Special
NS9	USOC and FID for combined XLL and NAB (same customer) (Listings)
NSEP	National Security Emergency Preparedness, National Security Emergency Procedures
NSH	USOC and FID for combined XLL and FNA (different customer) (Listings)
NSL	Number of Secondary Locations
NT1	Network Termination Device (ISDN)
NTAS	Nevada Trouble Analysis System
NTN	New Telephone Number
NTW	Network Terminating Wire
NWC	USOC for Network Change Charge (Business Hunt Group)
NWCLG	USOC for Network Change Charge
NWCPS	USOC for Network Change Charge
NWCRR	USOC for Network Change Charge (Residence Hunt Group)
NWP	National White Pages
NWPD	National White Page Directory; National White Pages System
NXX	3-Digit prefix of a telephone number or account (Central Office codes)
NYPS	National Yellow Pages Systems
OA	Operator Assistance
OAI	Open Access Interconnection
OANAD	Open Access Network & Development
OBF	Ordering and Billing Forum
OCA	Optional Calling Area Compensation
OCN	Operating Company Number
OPC	Originating Point Code
ORT	Operational Readiness Test
OS/DA	Operator Services and Directory Assistance
OSS	Operations Support Systems
P/L	Port/Loop Indicator
PA	Payments Applied

PACS Personal Access Communications System (wireless)

PALS Public Access Line Service (connects coinless public telephone dial tone in CO)

PAP FID for Prearranged PIN (calling cards); Public Safety Answering Point (E9-1-1)

PARIS Purchase of Accounts Receivable Information System (SWBT)

PATH QTY Path Quantity (DNCF)

PB Pacific Bell

PBCC Pacific Bell Cross Connect

PBCM Pacific Bell Call Management

PBD Pacific Bell Directory; Preferential Bill Date

PBITS Pacific Bell ISDN Test System

PBMS Pacific Bell Mobile Services

PBNI Pacific Bell Network Integration

PBOD Pacific Bell Operations Dispatch

PBOS Pacific Bell Operator Services

PBSM Pacific Bell Service Manager

PBVM Pacific Bell Voice Mail

PBVS Pacific Bell Verification Service; Pacific Bell Verification System

PBVS-LID Pacific Bell Verification Service—Line Information Database

PBX Private Branch Exchange

PBY Pacific Bell Yellow (pages)

PCA Protective Connecting Arrangement

PCO FID for Plant Control Office (special access)

PCS Personal Communications Services

PD Past Due

PDAC Planning Design Access Code; Power Distribution Alarm Control (private line services)

PDC Power Distribution Center; Primary Domain Controller

PDF Portable Document File (file created in Acrobat software); Prefix Data File (code openings); Protector Distribution Frame (in Central Office)

PDN Primary Directory Number

PDP Private Dial Plan

PDR Published Directory

PDT Plant Test Date

PEPC Post-Extraction Print Change (PBD closing)

PFA Product and Feature Availability

PFX Prefix

PH Primary High (E9-1-1 trunk)

PI Primary Rate Interface (ISDN); Professional Indication (White Pages)

PIC Point in Call; Predesignated Interexchange Carrier; Presubscription Indicator; Primary Interexchange Carrier

PIL Percent InterLATA

PIU Percent Interstate Usage

PIUM Percent Interstate Usage Measurement

PL Private Line

PLC Printer Listing Change (PBD)

PLD Primary Line Designation (OCP)

PLN Private Line Number

PLOC Previous Location

PLU Percent Local Usage; Percent Local Usage (% local minutes & % local messages)

PM Phase Modulation; Primary MPOE

PMC Public Mobile Carrier

PN Pilot Number (BTN) (first number in a number group); Primary Number

PNL Primary Node Link (SONET)

PNP Permanent Number Portability

POC Point Of Connect; Point Of Contact

POE Packet Office Equipment

POF Pending Order File

POI Point of Interconnection

PON Purchase Order Number

POP Point Of Presence

POT Point Of Termination

POTS Plain Old Telephone Service

PPD Preferred Payment Date

PPI Planning Provisioning Interface

PPS PCS Service Provider; Permanent Signal Partial Dial; Public Packet Switching; Public Packet Switching Network

PR Priority Ringing

PRA Preliminary Rate Authority; Primary Directory Alpha; Primary Rate Access

PRAF Pacific (Bell) Remote Access Facility

PRI Primary Rate Interface

PRICE Primary Directory Classified

PRIG Priority Ring

PRO Proof (SOD)

PROS Personalized Response System (Operator Services)

PS FID for Permanent Special Handling (calling cards); Permanent Signal; Port Service

PSAP Public Safety Answering Point

PSCN Public Service Commission Nevada

PSDS Public Switched Digital Service

PSN Public Switched Network

PSP Payphone Service Provider (formerly known as COPT [Customer Owned Pay Telephone])

PSS Pay Station Service Charge; Public Service Center

PST Public Switched Telephone Network

PTN Pending Transaction File; Pilot Telephone Number; Plant Test Number; Public Telephone Network

PTR Percent Traffic Routed; Poor Transmission

PTS Public Telephone Service

PTVS Pacific Telesis Video Services

PTW Public Telephone Network (traffic network providing PTS)

PU Public Utilities

PUC Public Utility Commission; Public Utilities Commission

PURA Texas Public Utility Regulatory Act of 1995

PVC Permanent Virtual Circuit (PL)

PVL Local Private Line

PVN Private Virtual Network

PZN Personalized Telephone Number

QDT Quick Dial Tone

QTY	Quantity
QUE	Queuing
R-EASE	Residential Easy Access Sales Environment
R-STC	Residual-Servicing Test Center
R/WCC	Radio/Wireless Common Carrier
RA	Recorded Announcement
RACF	Remote Access to Call Forwarding
RADN	Remote Access Dialing Number
RADR	Receiver Attachment Delay Recorder
RAF	SWBT Remote Access Facility
RAL	Resale Access Line
RALMB	USOC for Resale Access Line Multi-Line Business
RALMH	USOC for Resale Access Line Multi-Line Business Handicap
RALRH	USOC for Resale Access Line Residence Handicap
RALRR	USOC for Resale Access Line Residence
RALSB	USOC for Resale Access Line Single-Line Business
RALSH	USOC for Resale Access Line Single-Line Business Handicap
RAM	Random Access Memory; Resale Account Manager
RAO	Revenue Accounting Office
RAO-MDR	Revenue Accounting Office via Message Detail Recording
RATE	Resale Access to Exchange (CABS to CRIS)
RBOC	Regional Bell Operating Company
RC	Recurring Charges
RCC	Radio Common Carrier
RCD	USOC for restoral charge for SNP'd account
RCF	Remote Call Forwarding
RCFCH	USOC for change charge for RCF service
RCL++	Class of Service USOC for Residence loop
RCLO	Related Circuit Layout Order Number (TIRKS)
RCSR	Radio Carrier Service Request
RCVR	Receiver
RDBMS	Regional Database System
RDBS	Routing Data Base Systems; Routing Database System

RDVM	Remote Data Voice Multiplexer
REC	Record
RECCKT	Related Exchange Company Circuit Identification
RECFM	Record Format
REF NUM	Reference Number
REL	Resale Message (SS7)
REN	Ringer Equivalence Number
REPL IND	Replacement Indicator (indicates USOC being replaced by another USOC)
REQTYP	Requisition Type & Status
RESP ORG	Responsible Organization (custom 800 service)
RF	Radio Frequency (wireless)
RFF	Request For Feature
RFI	Request For Information
RFP	Request For Proposal
RFQ	Request For Quote
RGT	Record Group Table (code openings)
RI	Routing Index
RI-PH	Route Index Portability Hub
RIC	Residential Interconnection Charge; Residual Interconnection Charge
RID	Record Issue Date (FID)
RL	Loop with Reuse
RLC	Release Complete Message (SS7)
RLT	FID and USOC for Additional Residence Listing
RMAS	Remote Memory Administration
RMB	Remote Make Busy
RMI	Resale Mechanized Interface
RMKS	Remarks
RMV	Remove
RO	Related Order
ROAR	Resale with Operator Alternate Routing
ROC	Regional Operation Center
ROCC	Radio Operation Control Center (Mobile Services)

ROCP	Residence Optional Calling Plans
ROH	Receiver Off Hook
ROM	Read Only Memory
ROP	Receive Only Printer
RORD	Related Order Number
ROW	Right(s) Of Way
RPCU	Radio Port Control Unit (Wireless)
RPM	Rate Point Master file (provided by Bellcore)
RPON	Related Purchase Order Number
RRD	Rate Center Record; Requested Response Date
RRSO	Reuse with Related Service Order (cable & pair)
RRUD	Residence Resale Usage Discounts
RSA	Rural Statistical Area (wireless)
RSAP	Resale Service Area Plan
RSC	Remote Switching Center
RSLE	FID foresale
RSM	Remote Switching Module
RSP	FID for Rate Stability Plan
RSPPS	Rate Stability Payment Plans
RSS	Remote Switching System
RSU	Remote Switching Unit
RT	Remote Terminal
RTA	Remote Trunk Arrangement
RTAD	Remote Test Access Data
RTAP	Remote Test Access Placer
RTC	Remote Terminal Concentrator
RTG	Routing
RTN	Recording Telephone Number
RTP	Release To Pivot (LNP)
RTS	Repair Transfer Service; Return To Service
RTU	Radio Telephone Utilities
RUF	Reuse of Facility
RUM	Reseller User Migration
RVR	Multi-party service (ALRU-LMOS)

RW2	USOC for Rearranging inside Wiring
RWW	USOC for Rearranging Wiring (outside)
S & F	Services and Features
S&E	Service and Equipment
S60	Saver 60 (usage discount plan)
SA	Service Address; Special Access
SA1	First line of special calling card address
SA2	Second line of special calling card address
SAC	Service Area Code; Special Access Code
SAD	Service Address Directory; Service Address
SAG	Street Address Guide; Service Address Guide
SAI	Service Area Interface
SAP	Special Access POTS Service (Loop)
SATD	Street Address Telephone Directory
SB	Summary Billing
SBA	USOC for Special Billing Arrangement Charge
SBACO	USOC for Special Billing Arrangement Charge for CO work
SBC	Southwestern Bell Company; Subsequent Billing Company
SBI	SONET-Based Interface (SWBT)
SBILLNM	Secondary Billing Name
SBN	Special Billing Number
SBO	Single Bill Option
SBOG	Summary Billing
SC	Special Condition (listings); Special Construction requirement; Speed Calling
SCA	Selective Call Acceptance
SCC	Service Control Center; Switching Control Center
SCCP	Signaling Connection Control Point
SCE	Service Creation Environment (AIN)
SCF	Selective Call Forwarding
SCFA	Secondary Connecting Facility Arrangement
SCL	Speed Calling (long list); Subscriber Loop Carrier
SCP	Service Control Point
SCR	Selective Call Rejection

SCS	Speed Calling (short list)
SCTT	Station Call Through Test (Centrex)
SD	Service Date (due date); Subsequent (due) Date
SDN	Secondary Directory Number
SDS	Switched Digital Services
SDS56	ISDN Switched 56
SDSEC	Street (address) Directory Street Code
SDT	Soft Dial Tone
SE	Sonet Extender
SECAB	Small Exchange Carrier Access Billing
SECLOC	Secondary Location
SECNI	Secondary Network Channel Interface Code
SECTLV	Secondary Transmission Level Point
SEF	Switched Entrance Facility
SEG	Segment Number
SEP	Signaling End Point
SEQ	USOC for out-of-sequence caption listing charge
SF	Signal Frequency; Simulated Facility; Super Frame (ISDN)
SGN	Segment Number (FID required on multipoint circuits)
SHU	Stop Hunt
SI	FID for Service Inquiry; Switch Interface
SIC	Special 800 Service Code; Standard Industrial Classification (code)
SID	FID for Scheduled Issue Date
SIG	Support Implementation Guide
SIRD	FID for Service Inquiry Reply Date
SL	Secretarial Line; Signaling Link Transport
SLA	Secondary Location Address (Centrex only); Service Level Agreement
SLC	Structure License Coordinator (Right of Way); Subscriber Loop Carrier
SLCC	Standard Line Class Code (SWBT)
SLDB	Service Location Database
SLRCF	Single Line Remote Call Forwarding

SLV	Service Location Validation (Access To Information [CESAR])
SM	Secondary MPOE; Single Bill—Multiple Tariff (Meet Point Billing); Sonet Multiplexer
SMDR-P	Station Message Detail Recording to Premises (Centrex)
SMDU	(Pacific Bell and Nevada Bell) Statewide Marketing Directory Unit for Complex Caption Listings
SME	Subject Matter Expert
SMR	Specialized Mobile Radio
SMS	Service Management System; Service Management System (support system for 800 number translations)
SMS/800	Service Management System/800 Database (database used by all 800 service nationwide)
SMX	Sonet Multiplexer Xtra
SN	Subscriber Name
SNAP	Single Network Access Point
SNCC	Signaling Network Control Center
SNI	Standard Network Interface
SNID	SONET Network Identification (6-character identifier)
SNP	Suspend for Non-Payment
SNP/REST	Suspend for Non-Payment Restored
SNPA	Special Numbering Plan Area
SNTRNG	SONET Ring
SO	Service Order
SONET	Synchronous Optical Network
SORD	Service Order Retrieval and Distribution
SP	Saver Plus (Usage Discount Plan); Signaling Point; Single Bill—Pass Through (Meet Point Billing)
SPA	FID for Special Attention Required; Special Action Indicator
SPACC	Special Access (ALRU-LMOS)
SPB	Special Billing
SPC	Signaling Point Codes
SPC	Speed Calling
SPLNP	Service Provider Local Number Portability
SPNP	Service Provider Number Portability
SPOC	Single Point Of Contact

SPOI Signaling Point Of Interconnection; Single Point Of Interface

SPOT Secondary Location Point Of Termination

SR Selective Routing; Service Request; Special Routing Code; Sub Ready; Surcharge

SRA Special Rate Area

SRAS Special Routing for Access Service

SRN FID for Service Representative Name

SRVT SCCP (Signaling Connection Control Point) Routing Verification Test

SS Single Bill—Single Tariff (Meet Point Billing); Special Services

SS7 Signaling System 7

SSA Specialized Service or Arrangements; Standard Serving Arrangement

SSC Special Services Center

SSC/R-ST Special Services Center/Residual-Serving Test Center

SSD Special Services Dispatch

SSE Special Services and Equipment

SSFS Special Services Forecasting System

SSI&M Special Services Installation & Maintenance

SSM Sales Support Manager

SSMDP Special Services Mechanized Design Process

SSN Switched Services Network

SSP Service Switching Point; Shared Service Provider

SSPSC Special Services Plant Service Center

ST Selective Transfer (SWBT); Start (Signaling)

STC Service Test Center

STM SONET Terminal Multiplexer

STN Screening Telephone Number

STN Service Transport Node

STP Signaling Transfer Points; Signal Transfer Point (packet switch in Intelligent Network that routes signaling messages to other switching systems)

STPS Signaling Transfer Point Switch

STS-N Synchronous Transport Signal

STWRT Starwriter

SUP	Supplement Type
SUR	Summary Usage Record
SUS	(Temporary) Suspension at Customer's Request
SV	Signal/Voice path
SVC	Switch Virtual Circuit
SVGPFX	Serving Group Prefix
SVL	Supplemental Address Validation
SVP	Signal Voice Path
	Southwestern Bell InterConnect Agreement
SWBT	Southwestern Bell Telephone; Southwestern Bell Telephone
SWBT-CAT	Southwestern Bell Telephone Credit Card and Third Number System
SWC	Serving Wire Center
SWF	Switched Entrance Facility
SWF-DS1	Switched Functional DS1 Service Capability
SYNCH	Synchronous
T&F	To and From orders
T&M	Time and Material
T-1	(DS1 Loops) Provides a 4-wire facility capable of transporting 1.544 Mpbs DS1 digital service between two 4-wire interfaces
T-I AM	Timer-Initial Address Message
T-R	Tip and Ring
T/O	Terminating and Originating
T1SHC	T1 Carrier for Switched HICAP
TA	Trouble Administration; Terminal Adapter (ISDN)
TAAS	Trunk Answer Any Station
TACD	Telephone Area Code Directory
TAG	Translation Group; Trunk Assignment Group
TAR	Tax Area
TAS	Tandem Access Sectorization; Telephone Answering Service
TASC	Telecommunications Alarm Surveillance and Control
TASI	Time Assignment Speech Interpolation
TBCC	To Be Called Cut

TBE Toll Billing Exception

TC Transfer of Calls

TCA Tandem Completing Area

TCAP Transaction Capabilities Action Part; Transaction Capabilities Application Part; Transaction Capabilities Application Part (SS7)

TCAS T-1 Carrier Administration System

TCAT Telephone Number Category (PREMIS code for class of service)

TCC Telecommunications Code; Transfer Call Change

TCI Telephone Company Identification

TCIC Trunk Circuit Identification Code

TCIF Telecommunications Industry Forum

TCIS Transaction Communications Interface Subsystem

TCLR Terminating Carrier Common Line Rate

TCP Transfer Call Period; Transmission Control Protocol

TCP/IP Transmission Control Protocol/Internet Protocol

TCSI Transaction Code Status Indicator

TD Order Taken Date; Test Details

TDD Telecommunications Devices for the Deaf

TDM Time Division Multiplexing (HI-CAPS)

TDMA Time Division Multiple Access (PCS)

TE Tax Exempt

TEA Terminal Address

TEO Telephone Equipment Order

TER Terminal Number

TES Telephone Exchange Service

TESP SWBT's Technical Exhibit Settlement Procedures; Technical Exhibit Settlement Procedures

TFC Traffic

TFCDB Toll Free Calling Database

TFN To/From Number

TFRD Trouble Report Format Definition

TG Trunk Group

TGAC	Trunk Group Access Code
TGID	Trunk Group Identifier
TGN	Trunk Group Number
TGSR	Trunk Group Service Request
TH	Terminal Handler; Trouble History
THP	Terminal Handling Processor
TIA	Telecommunications Industries Association
TIC	Tandem Inter-LATA Connecting Trunk
TIRKS	Trunk Integrated Records Keeping System
TIRMS	Technical Information Reference Management
TLI	FID for lead number in a hunt group
TLN	Telephone Line Number
TLP	Transmission Level Point
TLWS	Trunk and Linework Station
TM	Transport Mileage
TMF	Transaction Monitoring Facility
TMG	Timing Source Indicator
TMNSXX	Line USOC for DID (PBX) trunks
TN	Telephone Number; Trunk Number
TNA	Telephone Number Assignment
TNC	FID for transfer of calls
TNC OPT	Transfer of Calls Options
TNC PER	Transfer of Calls Period
TNCTO	Transfer of Calls To
TNDNC	Tandem Demand and Capacity
TNI	FID for TIRKS Not Involved
TNLPC	Temporary No Late Payment Charge
TOD	Time Of Day
TOPS	Traffic Operator Position Systems
TOR	Terminal Owning Region
TP/DE	Toll Processing/Data Exchange
TPAD	Terminal Packet Assembler/Disassembler
TPB	Third-Party Billing
TPC	Terminating Point Code

TPCC Transport Cross Connect
TPG Terminating Point Group
TPI TIRKS/PICS Interface
TPIW Pacific Bell Placed Interior Wiring
TPM Terminating Point Masterfile
TPN Third-Party Notification
TPP Terminating Path
TQ Translation Questionnaire Request
TR Technical Requirements
TRA Bellcore's Traffic Routing Administration; Telecommunications Resellers Association
TRCC T-CXR (Carrier) Restoration Control Center; Trouble Reporting Carrier Control
TRCO Trouble Reporting Control Office
TRD Time Release Disconnect
TRDIG Terminating Digits
TRF Transfer Feature
TRFTYP Traffic Type
TRG Technical Review Group (Bellcore)
TRID Traffic Record Issue Date
TRK GRP Trunk Group
TRK QTY Circuit Quantity
TRKS Trunks
TRN Trunk Number
TS Tandem Switching; Traffic Sensitive
TSA Tandem Serving Area; Technical Support Administrator
TSC Telemanagement Services Center; Two Six Code (code assigned to a switched access trunk group)
TSG Trunk Sub-Group
TSMT Trunk Side Message Trunk
TSP Telecommunications Service Priority; Tandem Switch Provider
TSPS Traffic Service Position System
TSS Trunk Servicing System
TST Tandem Switched Transport; Test Code

TT	Terminating Traffic; Touch Tone; Translation Transmittal; Transport Termination
TTC	Tandem Transit Charge
TTD	Trunk Type Description
TTE	Trunk Traffic Engineering; Trunk Traffic Estimating System
TTP	Transmission Test Position
TTRAN	Telecommunications Transmission
TTT	Transport Trunk Termination
TTU	Trunk Test Unit
TTY	Line of Information (Listing); Telecommunications Device for the Deaf (non-chargeable)
TU	Telecommunications Utility
TUF	Translation of USOCs and FIDS
TVN	Traffic Violation Notice
TVO	Tag Values Outputs (NDM)
TWC	Three Way Calling
TWLT	Trunk With Line Treatment (wireless)
TXEX	Tax Exempt
UA	Usage Assembly
UCD	Uniform Call Distribution
UCD-DMS	Universal Call Distribution—Digital Multiplex System
UCD-ESS	Universal Call Distribution—Electronic Switching System
UCT	Unbundled Common Transport (SWBT)
UDDA	Unbundled Digital Directory Assistance
UDT	Unbundled Dedicated Transport (SWBT)
UI	User Interface
ULS	Unbundled Local Switching (SWBT)
ULTS	Universal Lifeline Telephone Service
UNCL	Unclassified (ALRU-LMOS)
UNE	Unbundled Network Element
UNI	User to Network Interface
UR	Usage Rating
URL	Uniform Resource Location
US	Universal Service

US3WC	Usage Sensitive - 3 Way Calling
USCC	Unbundled Services Cross Connect
USCCS	Usage Sensitive Custom Calling Service (also known a Pay-Per-Use)
USO	Uniform Service Order; Universal Service Order
USOC	Universal Service Order Code
USTA	United States Telephone Association
UTM	USOC for Message Station Equipment Recovery Charge
UTR	Universal Tone Receiver
UTS	Unbundled Tandem Switching
UWALS	Universal WATS Access Line Service
V&H	Vertical and Horizontal Coordinates
VCI	Virtual Channel Identifier
VCS	Video Communications Services
VER	Version Identification
VF	Voice Frequency
VFG	Virtual Facility Group
VFL	Voice Frequency Line
VFN	Vendor Feature Node
VG	Voice Grade
VGIOT	Voice Grade Interoffice Transport (SWBT)
VIN	Virtual Intelligent Network
VIP GW	Video Information Provider Gateway
VIP SMS	Video Information Provider Subscriber Management System
VIT	Vehicle Information Terminal
VLR	Visitors Location Registry (wireless)
VMI	Visual Message Indicator
VMS	Virtual Memory System
VMWI	Virtual Message Waiting Indicator
VMX	Voice Message Exchange
VN	Version Number
VNF	Verification Not Forced
VOS	Virtual Operating System
VPP	Value Promise(tm) - Plus (Optional Calling Plan)

VRT	Virtual Remote Terminal
VRU	Voice Response Unit
VTA	Variable Term Agreement
VTAM	Virtual Telecommunications Access Method
VTE	Video Teleconferencing Service; Virtual Telephone Exchange
WA	Wideband Analog; Work Address (in ID section of SORD order); Work Authorization
WAC	Wide Area Calling
WACD1	Work Authorization Circuit Detail Link 1
WACD2	Work Authorization Circuit Detail Link 2
WAL	WATS Access Line
WALF	WATS Access Line Extension
WALS	WATS Access Line Service
WAN	Wide Area Network
WATS	Wide Area Telecommunications Service
WBIN	Wholesale Buyer Identification Number
WC	Wire Center
WCH	Wire Center Horizontal Coordinates
WCO	FID for Writing Control Office (Special Access)
WCSR	Wireless Carrier Service Request
WCV	Wire Center Vertical Coordinate
WD	Wideband Data; Wideband Digital
WDM	Wavelength Division Multiplexing
WFA	Work Flow Administration
WFA/C	Work Force Administration/Controller
WFM	Work Force Management
WFS	Frames Work Station
WGID	Work Group Identification
WHSL	Wholesale
WLL	Wireless Local Loop
WLNP	Wholesale Local Network Platform
WNO	Wrong Number
WP	White Pages; White Pages-Other
WPBX	Wireless Public Branch Exchange

WPL	White Pages Listing
WPN	Wideband Premise Network
WS	Wireless Service
WSO	WATS Serving Office
WSOP	Working Service On Premises
WSP	Wholesale Service Provider; Wireless Service Provider
WTN	Working Telephone Number
WVLR	Wireless Visitor Location Register
WWI	Wireline Wireless Integration
XLKBU	USOC for Business Loop
XLKRE	USOC for Residence Loop
XLL	USOC and FID for Line Of Information (Listing)
XMP	XMS-based Peripheral Module
XPAD	Packet Assembler/Disassembler Host or Terminal
XPT	Cross Point
Y6VCX	USOC for End of Issue Billing for CLT (Listings)
Y6VRX	USOC for End of Issue Billing for RLT
YP	Yellow Pages
YPH	Yellow Pages Heading
YPPA	Yellow Pages Publishers Association
ZBR	FID for Bill Round
ZBTSI	Zero Bit Time Switch Interface
ZCON	FID for OCN (Operating Company Number)
ZDC	FID for Distribution Code
ZDCAD	USOC for Direct Customer Access/Directory Information
ZFCD	FID for Frame Continuity Date
ZH	FID for Deaf & Disabled Account (discount)
ZMRC	FID for Missed Responsibility Code (MAC)
ZPOI	FID for POI information
ZUM	Zone Usage Measurement
ZX1LM	PBX Class of Service
a/n	Alpha Numeric
cgsa	Cellular Geographic Service Area
cmc	Cellular Mobile Carrier Cellular Mobile Carrier

emr	Exchange Message Record System
kHz	Kilohertz
kbps	Kilobits Per Second
mbps	megabits per second
x-CONN	Cross Connection
BC Generic	Business Continuation; Business Continuity
DR Generic	Disaster Recovery
HR GENERIC	Human Resources
JPEG	Joint Photographic Expert Group

Index

A

Administrative/Office Team, 250
Advanced Encryption Standard, 208
AES, *see* Advanced Encryption Standard
Agreements
    contracts and maintenance, 218
    wireless, 218
Asynchronous Transfer Mode, 4
ATM, *see* Asynchronous Transfer Mode
Automated Call Distribution, 138, 182, 266
Automatic Voice Network, 206
AUTOVON, *see* Automatic Voice Network

B

BIA, *see* Business Impact Analysis
Building Entrance Facilities, 110
Business Impact Analysis
    consultants, 5–8
    defined, 23–30
    planning of, 275–277

C

Cable Cuts
    handling, 188
    protection against, 193–196
Carbon Dioxide, 112
Central Office
    end office, 190–191, 198
    tandem, 190–192, 198
Channel Banks, 228
Command and Control, 210–211, 217, 220, 247, 252, 333–334
Communications Privacy, 104–106
Consultants, 5–8, 66
Crisis Management, 272, 304–305, 438
Critical Events Log, 154–155, 163, 253

D

Damaged Facilities Restoration Team, 251–253
Data, Collection of, 31
Data Communications, 29
Data Encryption Standard, 208
DCS, *see* Digital Cross-Connect Systems
DES, *see* Data Encryption Standard
Digital Cross-Connect Systems, 80, 109, 120
Disaster, Causes of, 2, *See also* Equipment, failure
    earthquake, 123, 145, 150
    flood, 39, 117, 123
    hurricanes, 161–163
    people, 126–127
    software, 119–120, 125, 134–135, 141, 189, 212–213
    water, 112–117
Disaster, Probability, 37, 69
Dry-Pipe Sprinkler System, 103, 113–114

E

EMT, *see* Executive Management Team
Erlang Theory, 191–193
Equipment, 28
    failure, 241–246
    inventory, 134–142, 136–139
    power breaker, 121–122
Executive Management Team
    evaluation of plan, 257–268
    responsibilities of, 153–154

F

Facilities Team, 248, 405
Failure Mode Effects Analysis, 67–72
    in cable cuts, 194
FDA, *see* Food and Drug Administration
Federal Financial Institution Examination Council, 356

FEMA, *see* Failure Mode Effects Analysis
Fiber Optics, 227
Financial Accounting, 35
Finance Team, 248
Fire Retardant Cable, 111
Floor Grid Diagrams, 141, 218
Fire Suppression Systems, 111
Food and Drug Administration, 291
Foreign Corrupt Practices Act, 287–289
Frame Relay, 224–225
Front End Processor, 221
Funding, 36–40

G

Gramm–Leach–Bliley, 291–293, 355–356

H

Halon, 113, 114–115
Health Insurance Portability & Accountability Act, 282–284, 331–335, 355
HIPAA, *see* Health Insurance Portability & Accountability Act
Hooper Doctrine, 353
Hub and spoke, 198–199
Human Resources Department, 216

I

Infrared Scanning, 118–119, 126
Internal Audit Department, 142, 346
Internal Revenue Service, 289–290, 312–322
International Standards Organization, 300–301
Internet, 227–228
Internet Protocol, 4
IP, *see* Internet Protocol
ISDN, 229
ISO, *see* International Standards Organization
Isochronous, 225–226

L

LAN Systems, *see also* Open Systems, 3, 106, 107, 110
Legal Department, 306–312
Legal Team, 249
Lightning
  checklist, 118

M

Mainframes, 4, 221
Management
  presenting, 8
  summary, 33
Medical Team, 249

N

National Association of Regulatory Utility Commissioners, 201
National Association of Securities Dealers, 278
National Fire Protection Association, 294

O

Occupational Safety and Health Act, 284–287
Off-Site Storage, 30
Open Systems, 3, 107, 223
Operating and Security Standards, 99–128
  communication privacy, 104–106
  open systems, 107
  physical, large installations, 102
  physical, small installations, 101
OSHA, *see* Occupational Safety and Health Act

P

Pandemic, 298, 325–330
PBX, 116, 124–127, 158, 193, 228–229
Personnel, 28
Phases, recovery plan, 5–10
Plan, *see also* Funding
  documentation, 133–162
  sample table of contents, 143–150
Plan, Evaluation of, 257–268
Point to Multipoint, 201, 204, 207–209, *see also* Wireless Services
Presentations
  final, 35–36
  management, 39–40
  purpose, 30–31
Private Lines, 224–225, 229, *see also* Telephone Services
Public Relations Team, 250
Public Utility Commission, 127–128
Purchasing Team, 417

Q

Questionnaires, 27, 31–32, 34

R

Recovery Scenarios, 152–164
Recovery Time Objective, 24

Risk Management Team, 248–249
Risk Monitoring, 277–278
Risk Priority Number (RPN), 68, 70–71
Routing
  alternate, 196–197
  diverse, 196–197

S

Sarbanes–Oxley, 298–299, 354–355
Seamless Solutions, 182, 184–189
SEC, *see* Securities Exchange Commission
Securities Exchange Commission (SEC), 287, 300
Security
  practices, 108–109
Smart Network, 230–231
Sneakernet, 140
Software
  disruptions, 189
  inventory, 141
  testing, 159
Software Response Team, 247
SONET, *see* Synchronous Optical Network
Synchronous Optical Network, 197, 226

T

T1, 396–398, 421, 470
Telecommunications
  hubs, 78, 80
  recovery team, 212, 213
  security practices, 108–109
  systems, 1, 103
Telecommunications team, 247
Telephone Sservice
  800, 106
  incoming, 107
Transportation Team, 250
Tropospheric Scatter, 206–207

U

Uninterruptible Power Supply/System (UPS), 100, 103, 117, 124, 127
UPS, *see* Uninterruptible Power Supply/System

V

Vendors
  escalation lists, 107, 216
  equipment contracts, 120–121
  inventory, 139
Voice Communications, 28–29

W

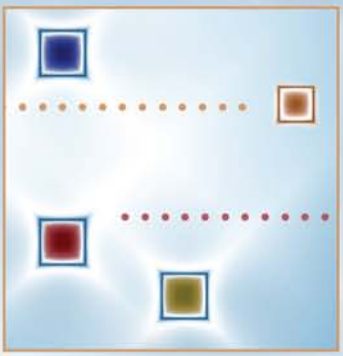
Water, *see also* Disaster, Causes of
  checklist, 118
  equipment room, 122
Water, Sources of, 116–117
Wireless Services, 201–209, *see also* Infrared
  microwave radio, 205–207
  satellite, 205–207

Information Technology

BUSINESS RESUMPTION PLANNING

Second Edition

Edited by LEO A. WROBEL



Offering hundreds of tips, templates, checklists, and pointers toward information in the public domain, ***Business Resumption Planning, Second Edition*** assists you in creating a rock-solid recovery plan for organizations of all sizes. It provides the information necessary for coordinating first responders to meet any disaster scenario head-on—whether it involves computers, telecommunications, or infrastructure—in a timely and effective manner.

What's New in the Second Edition:

- The latest techniques for conducting an efficient Business Impact Analysis and an accurate Failure Mode Effects Analysis (FMEA)
- Advice on how to successfully recover from "Ground Zero" events, such as the Oklahoma City bombing, 9-11, and Hurricane Katrina
- Tips for recovery teams and first responders, including how to maintain "4Ci" (Command, Control, Communications, Computers and intelligence) during a disaster
- An examination of legal ramifications resulting from a failure to plan—including new liability issues that directly affect you
- An explanation of how the Sarbanes–Oxley Act of 2002 impacts your planning efforts
- Plans and templates that assess vulnerability in WANs, Open Networks, physical facilities, environmentals, and enhanced services

To illustrate the vulnerabilities of today's mission-critical systems, this useful guide features actual case studies and examples, as well as a CD-ROM that contains worksheets, checklists, audit forms, work breakdown structures, and reports. With a clear, authoritative voice, this book details the proactive steps you should take now to first assess your exposure, then eliminate it.

CRC Press
Taylor & Francis Group
an informa business
www.taylorandfrancisgroup.com

6000 Broken Sound Parkway, NW
Suite 300, Boca Raton, FL 33487
270 Madison Avenue
New York, NY 10016
2 Park Square, Milton Park
Abingdon, Oxon OX14 4RN, UK

AU1459
ISBN: 978-0-8493-1459-9
90000
9 780849 314599

www.auerbach-publications.com