DISASTER RECOVERY PLANNING

Managing Risk and Catastrophe in Information Systems

Jon William Toigo

DISASTER RECOVERY PLANNING

Managing Risk and Catastrophe in Information Systems

Jon William Toigo

YOURDON PRESS
Prentice Hall Building
Englewood Cliffs, New Jersey 07632

LIBRARY OF CONGRESS
Library of Congress Cataloging-in-Publication Data

Toigo, Jon William
Disaster recovery planning : managing risk and catastrophe in information systems / Jon William Toigo.
p. cm. -- (Yourdon Press computing series)
Bibliography: p.
Includes index.
ISBN 0-13-214941-9 (Prentice Hall)
1. Electronic data processing departments--Safety measures. 2. Data processing service centers--Safety measures. 3. Disasters. I. Title. II. Series.
HF5548.2.T616 1989
658.4'78--dc19 88-20766
CIP

Editorial/production supervision and interior design: Elaine Lynch
Cover design: Ben Santora
Manufacturing buyer: Mary Ann Gloriande

A Division of Simon & Schuster
Englewood Cliffs, New Jersey 07632

The publisher offers discounts on this book when ordered in bulk quantities. For more information, write:
Special Sales/College Marketing
Prentice-Hall, Inc.
College Technical and Reference Division
Englewood Cliffs, NJ 07632

Printed in the United States of America
10 9 8 7 6 5 4 3 2 1

ISBN 0-13-214941-9

PRENTICE-HALL INTERNATIONAL (UK) LIMITED, *London*
PRENTICE-HALL OF AUSTRALIA PTY. LIMITED, *Sydney*
PRENTICE-HALL CANADA INC., *Toronto*
PRENTICE-HALL HISPANOAMERICANA, S.A., *Mexico*
PRENTICE-HALL OF INDIA PRIVATE LIMITED, *New Delhi*
PRENTICE-HALL OF JAPAN, INC., *Tokyo*
SIMON & SCHUSTER ASIA PTE. LTD., *Singapore*
EDITORA PRENTICE-HALL DO BRASIL, LTDA., *Rio de Janeiro*

Selected titles from the YOURDON PRESS COMPUTING SERIES
Ed Yourdon, *Advisor*

BLOCK The Politics of Projects
BODDIE Crunch Mode: Building Effective Systems on a Tight Schedule
BOULDIN Agents of Change: Managing the Introduction of Automated Tools
BRILL Building Controls Into Structured Systems
BRILL Techniques of EDP Project Management: A Book of Readings
CONSTANTINE AND YOURDON Structured Design: Fundamentals of a Discipline of Computer Program and Systems Design
DEMARCO Concise Notes on Software Engineering
DEMARCO Controlling Software Projects: Management, Measurement, and Estimates
DEMARCO Structured Analysis and System Specification
DICKINSON Developing Structured Systems: A Methodology Using Structured Techniques
FLAVIN Fundamental Concepts in Information Modeling
FRANTZEN AND MCEVOY A Game Plan for Systems Development: Strategy and Steps for Designing Your Own System
INMON Information Engineering for the Practitioner: Putting Theory into Practice
KELLER Expert Systems Technology: Development and Application
KELLER The Practice of Structured Analysis: Exploding Myths
KING Creating Effective Software: Computer Program Design Using the Jackson Method
KING Current Practices in Software Development: A Guide to Successful Systems
MAC DONALD Intuition to Implementation: Communicating About Systems Towards a Language of Structure in Data Processing System Development
MC MENAMIN AND PALMER Essential System Analysis
ORR Structured Systems Development
PAGE-JONES Practical Guide to Structured Systems Design, 2/E
PETERS Software Design: Methods and Techniques
RUHL The Programmer's Survival Guide: Career Strategies for Computer Professionals
SHLAER AND MELLOR Object-Oriented Systems Analysis: Modeling the World in Data
THOMSETT People and Project Management
TOIGO Disaster Recovery Planning: Managing Risk and Catastrophe in Information Systems
WARD Systems Development Without Pain: A User's Guide to Modeling Organizational Patterns
WARD AND MELLOR Structured Development for Real-Time Systems, Volumes I, II, and III
WEAVER Using the Structured Techniques: A Case Study
WEINBERG Structured Analysis
YOURDON Classics in Software Engineering
YOURDON Managing Structured Techniques, 3/E
YOURDON Managing the System Life Cycle, 2/E
YOURDON Modern Structured Analysis
YOURDON Structured Walkthroughs, 4/E
YOURDON Techniques of Program Structure and Design
YOURDON Writing of the Revolution: Selected Readings on Software Engineering
ZAHN C Notes: A Guide to C Programming

ACKNOWLEDGEMENTS

The author wishes to thank the following persons for their participation and support in the preparation of this book:

Mary Kern, her enlightenment born of experience, saw the need for disaster recovery planning and first placed me in the role of disaster recovery coordinator. She set the standards of performance by which I will judge myself for a very long time.

Judith Brugner, John Flint, Joan Kobernick, Tom Little, Ross Markley, Pat O'Connell, Judy Ryan, and the staff and membership of the Disaster Avoidance and Recovery Information Group provided observations and ideas that contributed much to the practical value of this book. The contributions of vendors and friends Steve Glantz, Kevin Hephner, and Mark Sher also deserve special note.

Edward Yourdon, Edward Moura and Patricia Henry are owed my deepest thanks for their steadfast belief in, and improvement of, both the author and the work.

Special thanks to Gary Eng, Mark Shulman, and Dennis Rapp of DataSouth, Inc., whose speedy and effective repairs to my PC averted the disaster of an unfinished manuscript and missed deadline.

Last but not least, my thanks and love to Jolanta, Alex, Max, and the entire Toigo and Suziedelis clans, who offered their support and encouragement. Without you, my dear family, this project would not have been completed.

MANAGEMENT OVERVIEW

The essence of good management is the rational, cost-effective use of resources. Next to personnel, a company's most important resource is information. Effective management of the information resource in a business enterprise is, therefore, a primary determinant of business success.

What does effective management of information mean? Today, the concept has become inexorably linked to the development, implementation, and refinement of technological tools for collecting, processing, and distributing information in a timely way. Effective information management has become synonymous with information systems management.

Information systems are now a basic component of nearly all business organizations. U.S. companies spent close to $30 billion on their information systems in 1987, and are reaping the fruits of their investments in the form of faster, more refined, more meaningful data—the kind of data that supports decisions and creates wealth.

However, there is a side to this symbiosis of business and machine that is rarely examined. It is business's dependency on the uninterrupted flow of information from its systems and the consequences to a company if the corporate oracle, the computer, were to be suddenly turned off.

These are the statistics:

1. The average company will lose 2-3 percent of its gross sales within 8 days of a sustained computer outage.
2. The average company that experiences a computer outage lasting longer than 10 days will never fully recover. 50 percent will be out of business within 5 years.
3. The chances of surviving a disaster affecting the corporate data processing center are less than 7 in 100. The chances of experiencing such a disaster are 1 in 100.

Despite these statistics and the numerous accounts of actual disasters that support them, many companies have ignored their vulnerability to a disastrous interruption of normal information system function. It was reported in 1986 that as many as 250 of Fortune 1000 companies had never planned for the possibility of an information system failure. The number of smaller companies without a disaster recovery plan is impossible to calculate.

In the financial industry, on the other hand, there has been a substantive trend toward disaster recovery planning. This trend has been spurred by federal and state legislation requiring the development and regular testing of disaster recovery plans. New laws have made bank managers and boards of directors personally liable for a failure to plan measures for reacting to, and recovering from, information system disasters.

Besides the frightening statistics and legal liabilities, there are other compelling and positive reasons to prepare contingency plans to protect corporate information resources. For one, disaster recovery planning can reduce corporate business interruption insurance premiums by 10 to 20 percent. This is because the planning process enables insurance requirements to be more accurately identified. In many cases, expensive blanket coverage can be replaced by more targeted policies.

In addition, many capabilities, such as uninterruptible power, that may be purchased for purposes of disaster prevention, may actually improve overall day-to-day system performance. Environmental maintenance can prevent costly equipment downtime as well as contamination-related equipment fires.

However, the ultimate impetus for disaster recovery planning is not financial. Disaster recovery planning is, after all, an overhead expense which demonstrates its worth in "non-events"—disasters that are prevented.

In the end, disaster recovery planning needs to be undertaken because of what it is: a fundamental component of effective resource management, the protection of vital corporate assets.

CONTENTS

Chapter 1

Introduction

The history of business automation is fascinating and vast. For the purposes of this study, however, one aspect of the history is especially important. Driven by the incentives of cost-efficiency and competition, business has placed more and more of its critical information asset into automated systems and networks. This, in turn, has made business dependent upon the uninterrupted function of the machine, a dependency rarely perceived by those within the corporation who have no direct contact with the data processing service. The consequences of a loss of information systems to the business may never be considered until a disaster occurs. By then, it is often too late.

Recent business experience is replete with examples of companies that failed to recover from a disaster. Some were consumed by a flood or fire that demolished offices and data centers, leaving skeletons of twisted metal and smoking rubble. Others died gradually over several years, after being crippled by a catastrophe from which they could never fully recover.

However, in the same historical experience there are also examples of companies that suffered disasters of the same magnitude and survived. They emerged from the crisis, with critical operations intact, to regain their position in the marketplace and to continue their commercial pursuits.

One must ask the reason for the different outcomes. Why do some companies survive when others fail? Is it simply fate or chance that determines success or failure in disaster recovery?

Disaster connotes chance or risk. The word itself is derived from the Latin word for "evil star." However, mounting evidence supports the fact that companies can take measures that will improve the likelihood of full recovery following a disaster. Put simply, the difference between winners and losers in a disaster is often the presence or absence of an effective disaster recovery capability. Companies that plan for the possibility of a disaster, that formulate strategies for recovering critical business functions, and that train employees to implement those strategies, generally do survive disasters.

This book is about disaster recovery planning. It is designed to equip a company contingency planner with the knowledge and skills needed to develop an effective disaster recovery capability. It is also intended to serve information systems managers and business executives as a primer

in the critical and often-rarified discipline of disaster recovery planning, and as a guide for managing the activities of the planning project. Finally, it is a pragmatic reference describing the products, practices, and politics of the disaster recovery industry that has emerged over the past two decades.

Having read this book, the reader will understand the principles of contingency planning and be equipped with a model of the planning project that he or she may emulate to develop a workable disaster recovery plan. Along the way, the reader will be exposed to some of the current debates and emergent technologies of disaster recovery as well as first-hand experiences of numerous business planners in both the preparation and implementation of disaster recovery plans. All that will remain is for the reader to select and apply what has been learned to develop a workable plan.

The term disaster, as used in this book, means the interruption of business due to the loss or denial of the information assets required for normal operations. It refers to a loss or interruption of the company's data processing function, or to a loss of data itself. Loss of data can result from accidental or intentional erasure or destruction of the media on which data is recorded. This loss can be caused by a variety of man-made or natural phenomena.

Loss of data can also refer to a loss of integrity or reliability either in the dataset (or database) itself, or in the means by which data is transported, manipulated or presented for use. Corruption of programs and networks can interrupt the normal schedule for processing and reporting data, wreaking as much havoc within a company as would the loss of the data itself.

The above conception of disaster may suggest that only a major calamity—a terrorist bombing, an earthquake, or even a war—would qualify as a disaster. One envisions a smoking data center at Goliath, Inc., rather than an accidental hard disk erasure at the small business office down the block. In either case, if the result is an unacceptable interruption of normal business operations, the event can be classified as a disaster. Disasters are relative and contextual.

However, there are some constants about disasters. One is time. Because of business's growing dependency on customized data processing systems, alternatives to system-provided functions and information cannot be implemented readily. Yet, for a business to survive a disaster, the time factor for restoration of system functions is critical.

According to a 1978 study by the University of Minnesota, a data processing failure in a financial institution, one-half day in length, will degrade normal business activity by 13 percent for the two weeks follow-

ing the failure.[1] A ten day outage will result in a 97 percent loss of business activity. Figure 1.1 depicts the impact of outages of varying lengths.[2]

The study also examined the relative vulnerability of specific industries and demonstrated the maximum downtime allowed by industry before recovery would be nearly impossible. As summarized in Figure 1.2, financial industries have the lowest tolerance to prolonged downtime, while insurance and manufacturing can tolerate slightly greater periods without business collapse.[3]

In manufacturing and distribution industries, however, even relatively brief outages entail substantial dollar losses. Figure 1.3 depicts the results of the 1978 analysis of dollar loss following a data center disaster in manufacturing or distribution industries with over $215 million annual gross sales.[4]

Although the Minnesota study is a decade old, experts still consider it to be an accurate portrayal of damage potentials confronting corporate data processing. However, the study did not account for the changes that have recently taken place in American business, including PC proliferation, the emergence of the private telecommunications switch, the growth of local area networks (LANs), and departmental computing. Thus, the study provides at best a conservative estimate of potential loss impact.

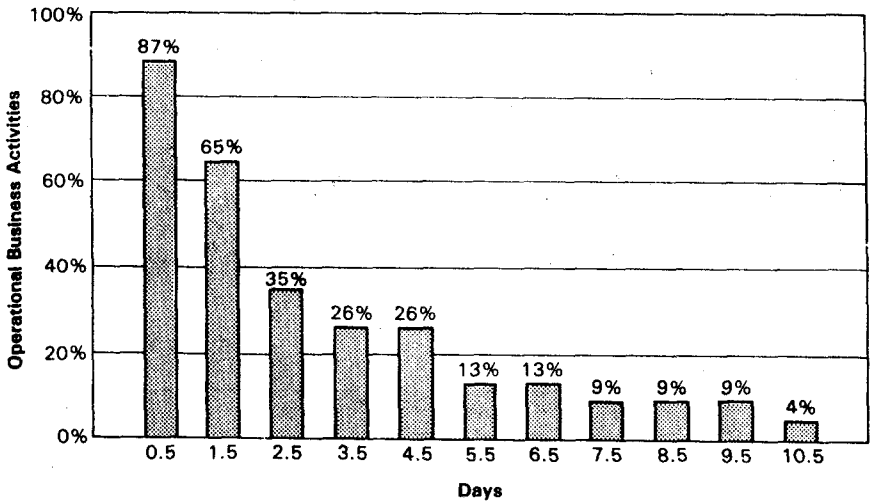


Figure 1.1 Decline in Operational Business Activities for the Finance Industry During the Two Weeks Following Complete Data Center Failure.

SOURCE: D.O. Aasgaard, et al., *An Evaluation of Data Processing "Machine Room" Loss and Selected Recovery Strategies* (Minneapolis; MISRC, University of Minnesota, 1979). Reprinted by permission.

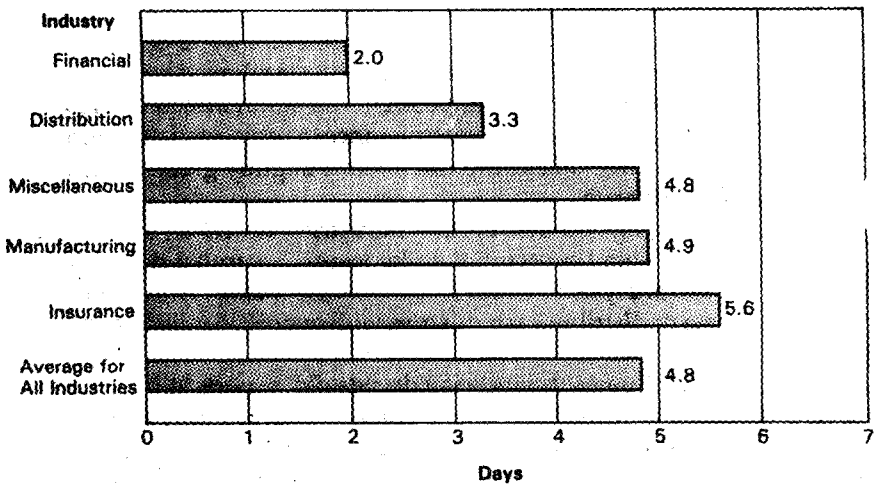
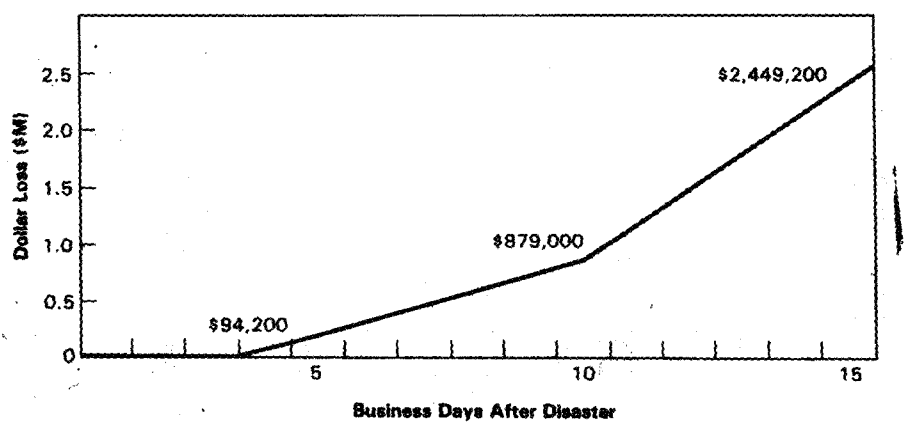


Figure 1.2 Maximum Downtime Allowed by Industry Type.
SOURCE: D.O. Aasgaard, et al., *An Evaluation of Data Processing "Machine Room" Loss and Selected Recovery Strategies* (Minneapolis; MISRC, University of Minnesota, 1979). Reprinted by permission.



(Based on Manufacturing or Distribution Industry with $215+ Million Annual Gross Sales)

Figure 1.3 Dollar Loss in Manufacturing or Distribution Industry Following a Data Center Disaster.
SOURCE: D.O. Aasgaard, et al., *An Evaluation of Data Processing "Machine Room" Loss and Selected Recovery Strategies* (Minneapolis; MISRC, University of Minnesota, 1979). Reprinted by permission.