

**NACRC ANNUAL CONFERENCE**  
**Philadelphia, Doubletree Hotel**  
**Monday July 16, 2001**

**BUSINESS CONTINUITY  
PLANNING**

**HOW TO DEVELOP A BUSINESS  
CONTINUITY PLAN**



Presented By  
**Ronald S. Rubino**  
**SouthTech Systems, Inc.**

600 West Santa Ana Blvd. #801  
Santa Ana, CA 92701  
(714) 972-8589  
[Ronr@southtechsystems.com](mailto:Ronr@southtechsystems.com)

**HOW TO DEVELOP A BUSINESS CONTINUITY PLAN**

**TABLE OF CONTENTS**

INTRODUCTION..... 3  
WHY SHOULD YOUR ORGANIZATION PREPARE FOR A DISASTER? ..... 3  
GETTING STARTED..... 4  
THREE PHASES OF BUSINESS CONTINUITY PLANNING PROCESS..... 5  
    • *Planning Phase (Pre-contingency)* ..... 5  
    • *Execution Phase (During Contingency)*..... 5  
    • *Recovery Phase (Post Contingency)* ..... 5  
PLANNING PHASE PRECONTINGENCY..... 5  
    *Step 1 Writing The Purpose, Objectives, Scope and Assumptions*..... 5  
    *Step 2 The Plan Coordinator and Development Team:* ..... 5  
    *Step 3 Assigning Action Items* ..... 5  
    *Step 4 Where Do You Stand Right Now?* ..... 6  
    *Step 5 Doing Your Business Impact Analysis* ..... 6  
    *Step 6 Selecting Your Recovery Teams* ..... 6  
    *Step 7 Developing Your Emergency Action Plans* ..... 7  
    *Step 8 Alternate Processing Locations and Service Vendors* ..... 7  
    *Step 9 Writing Your Business Continuity Plan*..... 7  
    *Step 10 Testing Your Plan*..... 8  
    *Step 11 Distributing Your Plan*..... 8  
    *Step 12 Maintaining Your Plan*..... 8  
FUTURE PLANNING EFFORTS..... 9  
    *Execution Phase During Contingency* ..... 9  
    *Recovery Phase Post Contingency*..... 9  
POTENTIAL CAUSES OF BUSINESS DISRUPTION..... 9  
PRECAUTIONS AND PREVENTIONS ..... 10  
RESOURCE GUIDE..... 11  
BIOGRAPHY..... 13

## **INTRODUCTION**

Whether it's caused by nature, technical problems or human error, any emergency can force catastrophic consequences and enormous costs on your government operations. The result: property damage, interruption of operations/processing, lost revenues, inability to meet legal requirements, frustration for customers and bad publicity about an elected official or government agency.

In emergency situations, it is critical that you make the right decisions and bring the immediate threat to the organization and its employees under control. Your organization must resume its most important functions in an emergency mode as quickly as possible. At the time of a disaster, the one thing that all organizations have working against them is time. Lost time translates into dissatisfied customers, lost revenue and more.

This report has been prepared for the County Recorders, Clerks and Election Officials as an introduction as to how to organize and undertake a comprehensive approach to business continuity planning and recovery. This report is designed to provide a “workbook” of ideas for the Department Head, Information Systems and operational staff to use when developing business continuity and resumption plans for their organization. This information is not intended to be a substitute for professional, technical, legal or financial advice needed to prepare a Business Continuity Plan.

## **WHY SHOULD YOUR ORGANIZATION PREPARE FOR A DISASTER?**

### What is Business Continuity Planning?

This is a planning process that can be under taken at the department or enterprise-wide level to ensure that an organization will remain able to perform its essential functions in the event of a disruption to normal business activities. In the business continuity planning process each organization must determine what are the priority functions and describe its business continuity measures. The resulting plans should describe the strategy, procedures and resources that will be utilized to enable the organization to continue essential processes regardless of whether or not systems are operational, facilities and infrastructure services are available, or other organizations are viable.

### Reasons for Having a Plan

These are just a few of the reasons why business continuity planning is necessary:

- Ensure the continuity of government services
- Protect the rights, property, health and safety of citizens
- Some problems will be overlooked, ignored, or work will not be completed on time if you do not plan in advance

## ***BUSINESS CONTINUITY PLANNING***

- There will not be enough money or time to fix everything in the short term back to the original state
- Planning ahead helps to prevent a disruption
- Exercising the plan allows for a test in controlled conditions and trains staff
- It is impossible to ensure that other organizations and groups both internal and external will have working systems
- The public need for services may be greater in a natural disaster
- Provides strategies for an organization to meet legal responsibilities
- Prevents loss of revenue
- Prevents loss of employee productivity
- Prevents loss of historical records of value and knowledge
- Avoids public embarrassment for official and government organization.
- Meets audit requirements to protect assets and preserve their viability

## ***GETTING STARTED***

### Basic Considerations

- Determine the scope of the plan(s)
- Define priorities and be sure all concern agree
- Establish responsibilities for developing and maintaining each business continuity plan
- Establish estimated length of time to prepare plan
- Determine whether internal and external resources are needed to prepare the plan
- Understand the planning effort will not be as effective if you do not commit to training staff, acquiring supplies, implementing preventative measures, exercising the plan and defining the period of time between major reviews and changes to the plan
- Obtain Information Technology Department's support and participation
- Obtain Executive Office approval and financial support

## **THREE PHASES OF BUSINESS CONTINUITY PLANNING PROCESS**

There are three phases to the business continuity planning process. The first phase is the focus of this report because it presents the process for the planning before a business disruption occurs. The preventive portion of Phase I will require the most effort to research information, analyze vulnerability and prepare a plan to deal with a range of potential business disruptions. The second and third phase deal with the execution of the plan due to a problem and the process of recovery after the incident has occurred and a stable operation has been re-established. The three phases of the business continuity planning process are:

- Planning Phase (Pre-contingency)
- Execution Phase (During Contingency)
- Recovery Phase (Post Contingency)

## **PLANNING PHASE PRECONTINGENCY**

### **Step 1 Writing The Purpose, Objectives, Scope and Assumptions**

- Purpose of the Plan
- Plan Objectives
- Scope of the Plan - Guidelines
- Planning Process Assumptions

### **Step 2 The Plan Coordinator and Development Team:**

- The Plan Development Team
- The Plan Development Team Roster
- Job Descriptions

### **Step 3 Assigning Action Items**

- Written Project Plan
- Coordination of Responsibilities and Time Frame
- Use of Intranet Web and Other Collaboration Tools
- Regular Status Report to Department Head

## Step 4 Where Do You Stand Right Now?

- Begin by Reviewing Existing Records Management and Disaster Recovery Plans and Policies
- Identify Codes and Regulations
- Identify Critical Products, Services and Operations
- Identify Your Internal Resources and Capabilities
- Identify External Resources
- Do an Insurance Review
- Prepare a Vulnerability Analysis
- Begin by Listing Potential Threats
- Estimate Probability
- Assess the Potential Human Impact
- Assess the Potential Property Impact
- Assess the Potential Business Impact
- Assess Internal and External Resources
- Compare Highest Risks With Preventive Action

## Step 5 Doing Your Business Impact Analysis

- Identifying Critical Systems, Applications and Vital Records
- Prepare Business Impact Analysis Department Questionnaire
- Discuss With Key Staff Business Impact Analysis Results
- What's Your Staying Power? ( <4 hours, < 8 hours, < 2days, >2days)
- Document Results
- Prioritize Your Defense

## Step 6 Selecting Your Recovery Teams

- Organization
- Responsibilities
- Team Assignment Call Sheet
- Internal Resources
- External Resources

## Step 7 Developing Your Emergency Action Plans

- Scenario 1 - Minor Damage/Disruption (facilities, computer room, servers, network, Internet connection workstations, peripheral equipment)
- Scenario 2 - Minor to Moderate Damage/Disruption
- Scenario 3 - Moderate Damage/Disruption
- Scenario 4 - Severe Damage/Disruption

## Step 8 Alternate Processing Locations and Service Vendors

- Alternative Office Locations With Department's Authority
- Internal Agreements For Mutual Aid
- Other Government Agreements For Mutual Aid
- Vendor Call Sheet

## Step 9 Writing Your Business Continuity Plan

- Executive Overview Of The Plan
- Recovery Team Structure
- Command And Control Information
- Critical Staff Members And Contact Information
- Emergency Evacuation And Security Procedures
- Alternate Site Locations And Preparations
- Listing Of Critical Business Functions
- Detailed Emergency Action Plans Including Temporary Operating Procedures
- Off-Site Storage Locations For Computer Backups And Critical Supplies
- Critical Forms And Supplies
- Asset Recovery/Salvage Procedures
- Inventory Of Critical Assets, Documentation, Supplies And Recovery-Related Inventories

## Step 10 Testing Your Plan

- **No test = no plan**
- Preparation of Testing Procedures
- Checklist Testing
- Non-Business Interruption Test
- Parallel Testing
- Business Interruption Testing
- Frequency of Test
- Evaluating Your Test Results
- The Checklist Worksheet
- Test Update and Problem Log
- Test Plan
- Test Evaluation Form and Guidelines

## Step 11 Distributing Your Plan

- Produce The Plan In A Binder For Ease Of Updating
- Plan Should Be Dated And Signed By Department Head
- Keep A Backup Copy At Home
- Keep A List Of Critical Telephone Numbers In Your Car

## Step 12 Maintaining Your Plan

- Assign As A Responsibility To A Management Level Person
- Develop A Business Continuity Plan Maintenance Sheet
- Conduct Security Audits And Document Results
- Conduct Data Backup Audits
- Inspect Annual Off Site Storage Of Records And Computer Backup Materials
- Update Names And Phone Numbers Semi Annually

## **FUTURE PLANNING EFFORTS**

### Execution Phase During Contingency

- Execute specific business continuity plans as required
- Notify appropriate authorities of nature and scope of problem
- Maintain manual logs
- Minimize threat to life and property
- Minimize damage to equipment
- Minimize damage to data
- Establish communications and management coordination process with support organizations
- Keep employees informed
- Keep the public informed through cooperation with media

### Recovery Phase Post Contingency

- Execute post-contingency plans as required
- Restore and restart systems as required
- Check system functions and results
- Correct and restore corrupt and or lost data
- Notify appropriate authorities of resolution of problem
- Modify and improve business continuity plan as required

## **POTENTIAL CAUSES OF BUSINESS DISRUPTION**

### Natural Disasters

- Hurricanes
- Tornadoes
- Floods
- Earthquakes
- Fire/Smoke
- Snow/Ice

### Facilities and Equipment

- Power Outage \*\*\*
- Water Leaks
- Equipment Failure
- Loss of Environmental Controls
- Interruptions of Internal/External Telecommunications\*\*\*

## ***BUSINESS CONTINUITY PLANNING***

### Software Problems

- Irrational or Unpredictable Results
- Irrational Data Presented to Users
- Files Corrupted or Lost
- Degradation of Performance
- System Hang-up or Shutdown

### People Caused Problems/Security Breach

- Human Error \*\*\*
- Terrorism
- Computer Virus \*\*\*
- Employee Caused Disruption
- Workplace Violence
- Citizen Caused Disruption
- Loss of Vendor due to Illness, Death or Failure to Perform
- Loss of Key Supplier
- Sabotage and Deliberate Infiltration or Attack on Critical Systems

\*\*\* Indicates a high percentage of disruptions are caused by this occurrence

## ***PRECAUTIONS AND PREVENTIONS***

- Backup Power Supply
- Data Backup And Offsite Storage Of Media
- Source Code Backup And Offsite Storage Of Media
- Automatic Remote File Copying
- RAID (Redundant Array Of Inexpensive Disks)
- Electronic Vaulting
- Security Policies And Procedures
- Network Monitoring Software And Reports
- Intrusion Detection Reports With System Generated Audit Logs
- Security Audits
- Antivirus Software
- User Access Control And Authentication
- Password Changes
- Smart Cards
- Encryption
- Digital Signatures
- Security Software
- Software Firewall
- Hardware Firewalls
- System Security Awareness Training
- Data Recovery Tests

## **RESOURCE GUIDE**

### **Resources**

Disaster Recovery Journal Magazine

[www.drj.com](http://www.drj.com)

Over 9,000 html files with search engine

Business Continuity Vendor Section

Products

Rothstein and Associates

The BCP industry's principal source for books, software, videos and research reports.

[www.rothstein.com](http://www.rothstein.com)

Fire Proof safes and cabinets

Schwab Corp.

P.O. Box 5088

Lafayette, Indiana 47903

800 428-7678

Arcus Data Security, Inc

Off-site Data Security and disaster recovery services

Disaster Recovery Kits

Arcus Data Security

800-GO-ARCUS

Disaster Recovery Institute (Canada)

PO Box 2911 Hamilton L8N 3R5, Canada

800 965-4608

<http://www.dri.ca>

**BUSINESS CONTINUITY PLANNING:**

**A STEP-BY-STEP GUIDE WITH PLANNING FORMS**

**(2000 EDITION - INCLUDES CD-ROM)**

**By Kenneth L. Fulmer, CDRP**

"This popular book gives you a comprehensive, step-by-step outline filled with precise instructions, risk and business impact analysis guidelines and forms for creating your business continuity blueprint. It serves as a workbook for those organizing a plan, and as a guidebook for those responsible for implementation. Clear and complete, Business Continuity Planning will prove an invaluable resource and guide for managers, owners and planning coordinators."

*BUSINESS CONTINUITY PLANNING*

EMERGENCY RESPONSE PLANNING FOR CORPORATE AND MUNICIPAL MANAGERS (1999 EDITION ISBN:0-12-241540-X)

By Paul A. Erickson Available from Academic Press (800) 321-5068

DISASTER RESOURCES GUIDE

P.O. Box 15243

Santa Ana, CA 15243

Santa Ana, CA 97235

(714) 558-8940

[www.disaster-resources.com](http://www.disaster-resources.com)

Annual guide to disaster resources for prevention, mitigation, response and recovery.

## **BIOGRAPHY**

### **RONALD S. RUBINO**

Ron Rubino is a Principal of SouthTech Systems, Inc. a systems development and consulting firm specializing in document management systems for public sector agencies. Ron worked for the County of Orange for 20 years and held senior level management positions in County government including Auditor-Controller's Office, Director of Information Systems, and CAO Director of Management & Budget. As Orange County's Director of Information Systems he was responsible for management of the County's data processing, telephone systems, and radio communications systems, with over 500 employees and \$50 million annual budget.

From 1994 to 1997 Mr. Rubino providing consulting services in areas such as process improvement, financial planning, information systems planning, systems development, and business continuity planning. From 1997 to 1998 Ron worked as the Director, Public Records Systems of Data Tree Corporation. In this capacity he was responsible for the marketing and customer service of document management systems to public agencies.

In 1998 Mr. Rubino became a Principal of SouthTech Systems, a software development firm located in Santa Ana. SouthTech Systems is the primary software firm to the Orange County California Clerk-Recorder' Office. They have developed an Internet Electronic Recording, Grantor/Grantee, Vital Records, Cashiering/Fee Accounting, Fictitious Business License, Marriage License System and 20-Day Notice Systems. SouthTech Systems also developed LASAR, a Legislative Action Storage and Retrieval System database and imaging automation for production of agendas and agenda action documents. SouthTech Systems also offers consulting services for IS Strategic Plans, business continuity studies, custom system development and outsourced programming services.

Mr. Rubino received his BS degree in Business Administration and Accounting from California State University Los Angeles. He earned a Master's Degree in Public Administration from California State University, Fullerton and completed the Executive Management Certificate Program at University of California Irvine. Ron has taught Public Administration and Business Administration courses at California State University, Long Beach Center for Public Policy and at the University of California Irvine.