



# Disaster Recovery Cookbook

Recipes for Small and Medium  
Enterprises

# So Who is This Guy Anyway?

## ◆ Founder and Chief Scientist

### Networks Are Our Lives, Inc!

- Network and Directory Services Design
- Backup and Disaster Recovery Planning
- Network Documentation
- Systems Management/Monitoring Deployment

## ◆ Author

- ◆ Over 100 articles and product reviews since 1987
- ◆ Currently writing:  
The Disaster Recovery Cookbook for Windows

## ◆ Contact:

Networks Are Our Lives, Inc!      hmarks@naol.com  
920 Hudson St.                      (866) 812-7611  
Hoboken, NJ 07030                      WWW.NAOL.COM



# First a few disasters:

## ◆ Natural

- Flood
- Storm (Hurricane, Tornado Etc.)
- Earthquake, Mudslide

## ◆ Man Made

- Fire, Explosion
- Power failure
- Hazmat

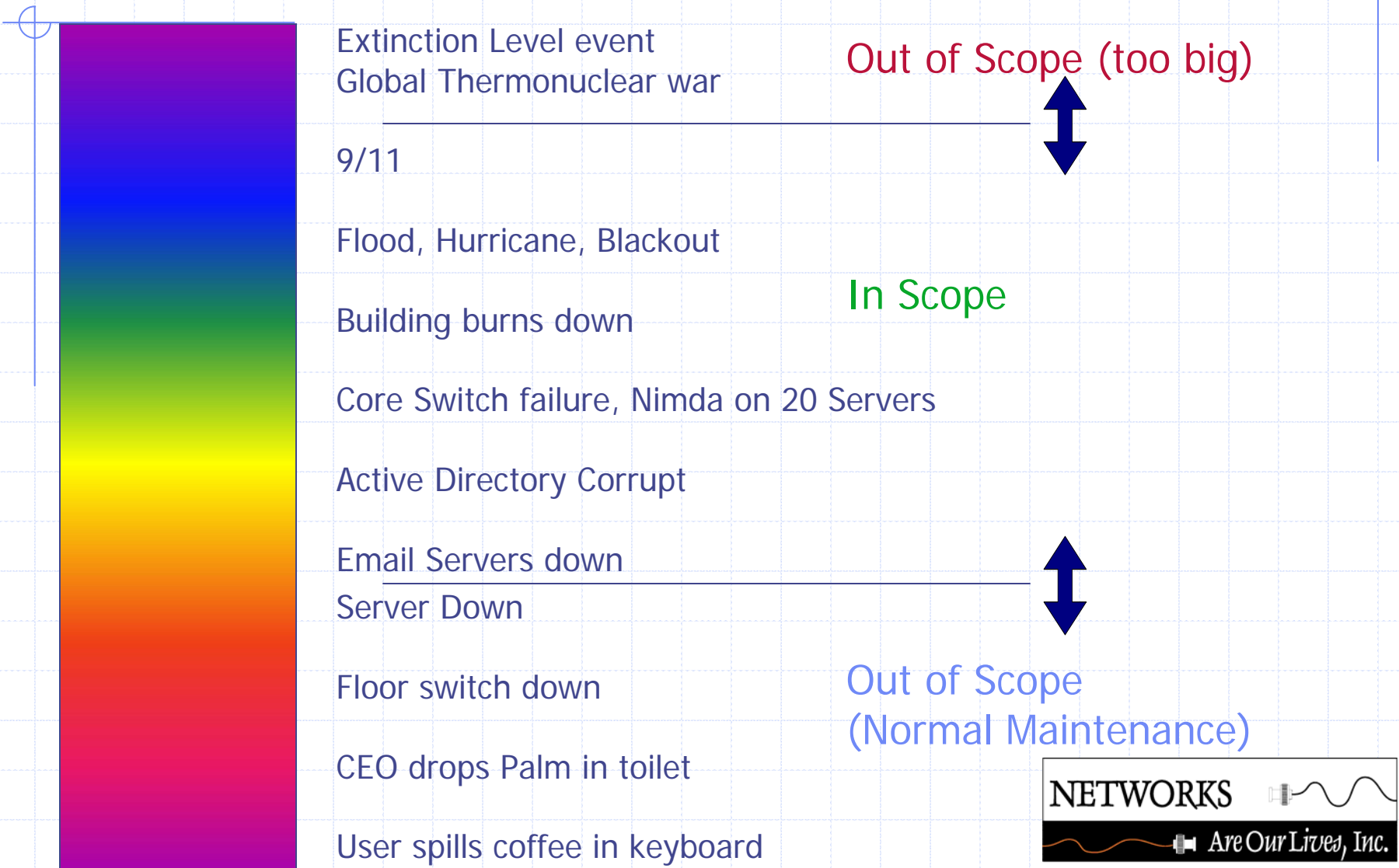
## ◆ Technological

- Virus, Worm other Malware
- Sabotage
- DDoS or other direct attack

# So What Do We Really Mean By Disaster

- ◆ An event which causes your IT services to be unavailable to your users
- ◆ The event is small enough that restoring the IT services is important
- ◆ The event is large and uncommon enough to rally extraordinary efforts and or resources
- ◆ Typically we plan for a data center being unavailable

# The Disaster Spectrum



# Important Thoughts

## ◆ "A Failure to Plan is a Plan to Fail"

- ◆ Legendary UCLA coach John Wooden

## ◆ "No Plan of Battle Ever Survives Contact With the Enemy"

- ◆ Credited to Field Marshall Helmuth Carl Bernard von Moltke, General George C. Marshall and Napoleon Bonaparte

## ◆ Which boils down to:

- You need a flexible plan

# Today's Problem

- ❖ Wall Street, due to legal mandates has real-time recovery for critical systems
  - Those solutions cost a minimum of \$300,000 plus \$50,000/mo
- ❖ Microsoft's definition of a disaster is a dead server
- ❖ So we know we need a plan and don't know where to start

# Recovery Elements

## ◆ Data

- On file servers
- In databases and message stores
- On local hard drives
  - ◆ Don't forget the laptops

## ◆ Application Availability

## ◆ User Work Environment

- Place to work
- Systems and applications
- Re-direct of phone numbers

# Disaster Avoidance

- ◆ Environmental control
  - Power
  - HVAC
- ◆ High availability systems
- ◆ System management
  - Patch management
  - Virus Protection
  - Decent Security Etc.
- ◆ A Quality Backup Process
  - HA could just propagate corrupt data

# The 9 Step Planning Process

1. Services Inventory
2. Risk Assessment
3. Assignment of Roles
4. Identify Possible Solutions
5. Choose Solutions
6. Implement Solutions
7. Create Recovery Manual
8. Test Recovery
9. Train, Maintain, Document

# Step 0. Selling Management

## ◆ Explain legal requirements

- Sarbanes-Oxley
- HIPPA
- SEC and other regulations

## ◆ Try FUD

- "X (60-90)% of all companies that suffer a disaster are acquired or out of business in 2 years"

## ◆ Auditor requirements

## ◆ Less of an issue in the post 9/11 world

# 1. Services Inventory

- ◆ Include ALL your technology services
  - Applications
  - Telephony, FAX Etc. not just applications
    - ◆ Circuit numbers, contact phones Etc.
  - Even the ones you claim not to support
  - Especially that HR app created and managed by consultants
- ◆ Get EVERYTHING needed to restore:
  - Serial Numbers/Key Codes Etc.
  - Collect installation media/data
- ◆ Be sure to identify dependencies

# Collect Data for Applications

**DRP Application Data**

Application Name: Quickbooks

Instance: Client ABC Co

Version: 2002

Business Group: Client Services

Business Owner (super User): John Sirica

Backup super user: John Dean

Technical Owner: Gordon Liddy

Backup technical owner: Bob Haldeman

Publisher: Intuit

Vendor: CDW

Who Provides Support: Intuit

Support Telephone Number: 1-800-555-1212

Support Type:  Free  Time and Materials  
 Contract  Paid Incident  
 Other \_\_\_\_\_

Contract/Incident account #: None

Contract exp. Date: \_\_\_\_\_

Maintenance Contract: (Y/N)    #    Exp

Date: \_\_\_\_\_

Architecture:  File  2 Tier Client/Server  
 Messaging  n-Tier Client Server  
 Web Tiers: \_\_\_\_\_ (1/2/3)

**File Based Application Data**

Application Install Point: \\DRFS\APPS\QB2002

Number of Licenses: 5

Type of license:  Perpetual  Concurrent  
 Workstation  Named User  
 Limited Time Expires: \_\_\_\_\_  
 Dongle Stored: \_\_\_\_\_

Install Codes/Serial Numbers:

1111-111-1112112	1111-111-1112113
1111-101-1112112	1181-111-1112112
1111-111-1192112	1811-111-1112112

Data Location (UNC): \\Clinetfs\ABC\ACCT

Drive Mapping:    Q: \_\_\_\_\_

OS Dependancies:  Windows NT 4 Service Pack: 6a  
 Windows 2000 Service Pack: \_\_\_\_\_  
 Windows XP Service Pack: \_\_\_\_\_

Installation Instructions:

Just run Setup


\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_


  
**Are Our Lives, Inc.**

# Rank Services and Applications

- ◆ Each service or application
  - Critical
  - Vital
  - Sensitive
  - Nice to have
  - Should be dead already
- ◆ Assign RTO, DLO to each category
- ◆ Survey users
  - Then add your expertise
  - Get Sr. management buy in for downgrades

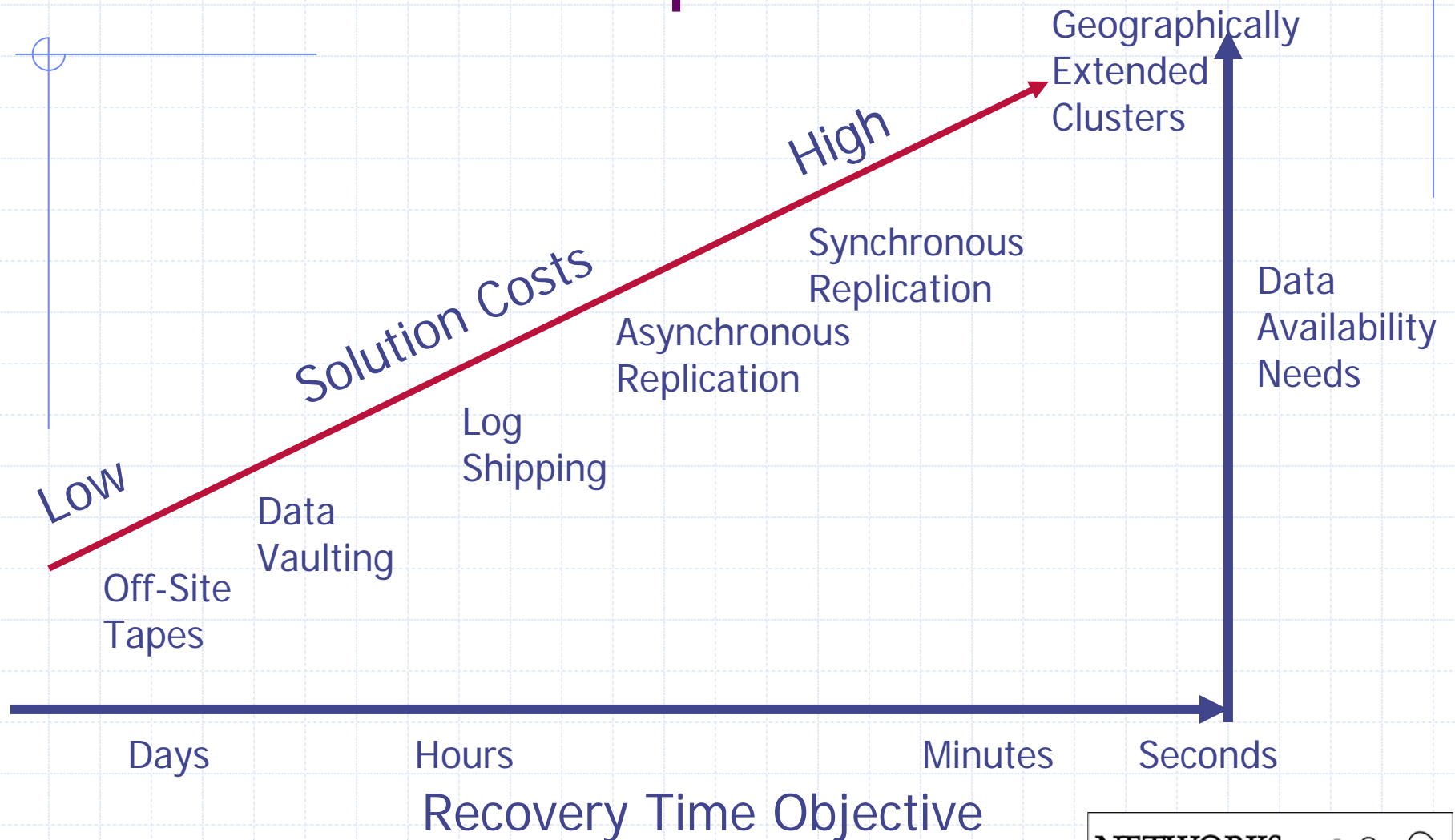
## 2. Risk Assessment

- ◆ Typically cost of downtime
  - Usually described as \$250,000-\$1,000,000/hr in lost revenue
  - Actually a step function times cost per user
    - ◆ 1<sup>st</sup> minute negligible cost
    - ◆ 3 months infinite cost
  - Include PR, customer relations impacts
- ◆ Add in cost to recreate data
  - Very application dependant
    - ◆ Amazon orders are lost and unrecoverable
    - ◆ I might need to re-write an article

# Define Objectives

- ◆ Recovery Time Objective (RTO)
  - Time between declaration and service availability
  - Think restore time
- ◆ Data Loss Objective (DLO)
  - Data in system at disaster time but not recovered
  - Think data entered since last backup

# The Solution Spectrum



# 4. Identify Possible Solutions

- ◆ Identify available solutions for each application or service
- ◆ Build a matrix of solutions that could meet various RTO, DLO and cost requirements
- ◆ Identify vendors for DR services
  - Server locations
  - User work area providers
  - Restoration help
  - Etc.

# Off-Site Tapes

## ◆ Send tapes off site

- You know you should but do you?
- How often?
- Where?
- If your data center is unavailable could you know what to recall?

## ◆ Records storage services

- Arcus (div. Of Iron Mt.)
- Recall
- Etc.

# Restoring From Off-Site Tapes

1. Get new server and tape drive
  2. Get backup software
  3. Install Windows Server & backup app
  4. Re-Catalog tapes
  5. Install Windows Server and backup agent on server to restore
  6. Restore data
- ◆ How long did this take?

# Data Vaulting

- ◆ Agent on server scans for changed blocks in files then sends them to vault
- ◆ Gets data offsite ASAP
- ◆ DLO reduced to hours
- ◆ If full restore needed vault vendor ships CD, DVD, Tape or NAS
- ◆ Costs from \$20/mo for 1GB to \$1000/mo for 50GB
- ◆ Providers:
  - Amerivault, Evault, LiveVault and many others

# Replication Solutions

## ◆ Synchronous

- Major SAN array vendors, NetApp Etc.
- Veritas Volume Manager
- Legato Co-Standby Server
- NSI Geocluster

## ◆ Asynchronous

- Veritas Volume replicator, Storage replicator
- Legato RepliStor (Formerly Octopus)
- NSI Double-Take
- Software Pursuits SureSync

# Where to replicate?

## ◆ In the array

- High performance
- Requires similar hardware

## ◆ Host based

- Can be application aware
- Could require multiple instances

## ◆ Replication/CDP appliance

- Can insure transaction integrity
- Usually requires Fibre Channel SAN

# Server location options

- ◆ DR provider
- ◆ Quick Ship
  - You'll need somewhere to ship to
  - Doesn't work if all aircraft grounded
- ◆ Collocation site
  - Typical Cost \$1000-\$2000/rack/mo
  - Includes bandwidth

# DR Services

## ◆ Recovery Work Space

- Ranges from desk and phone with PC to Specialized trading turrets and systems
- You pay per month plus per day after declaration

## ◆ Dedicated servers

- Servers for your use on line at site
- Yours or provided by vendor as part of contract

## ◆ "Shared" servers

- Vendors servers available to you after declaration and for testing
- You pay per month plus per day after declaration

## ◆ Quick Ship Servers

## ◆ Bandwidth

# DR Services Providers

## ◆ Full Service, National

- Sungard (including former Comdisco)
  - LIC, Carlstadt NJ
- IBM
  - Tuxedo Park NY
- HP

## ◆ Regional/Local

- Savvy Networks "The Bunker" Tarrytown

# 5. Choose Solutions

- ◆ Match solutions to RTO DLO of applications
- ◆ Decision order
  - Do my RTO and DLO allow restore from backup?
  - Do I want to manage servers myself?
  - Do I need 1 stop shopping?

# Virtualization can help

- ◆ Faster recovery of servers/apps
  - If not necessarily data
- ◆ Fewer servers to pay for at DR site
  - Can easily migrate VMs to additional servers after declaration

# Then start testing solutions

- ◆ Do they really work?
- ◆ Can your staff handle them?
- ◆ How much bandwidth will your applications need?
  - We test applications 1 at a time and monitor bandwidth usage
  - Email load generator helps
- ◆ Keep adjusting to balance against budget

# 6. Implement Solutions

- ◆ Now you get to find out how agents really effect production systems
- ◆ Monitor source servers and bandwidth usage as agents added

# 7. Create Recovery Manual

## ◆ Contents:

- Data from inventory
- Restore instructions based on selected solutions
- Contact list and call tree
  - ◆ Staff
  - ◆ Consultants and other vendors
- Disaster roles and procedures

# When writing remember

- ◆ Nothing you didn't write down to store off site is available
  - Installation CDs
  - Install Codes
  - IP addresses
- ◆ Write so ANY MCSE could follow
  - While Bill knows how to bring up WonderCalc he might have been in the building when it burned down
- ◆ Find someplace off site to keep the manual
  - Locker at DR site, data vault, Hosted website Etc.

# Any Questions?

