

DISASTER AVOIDANCE



Kristine Lindely – Enterprise Technologist

Is it Disaster Recovery or Business Continuity?

- Disaster Recovery (DR) - reactive:
 - The ability to restore an organization's critical business functions in the event of a business interruption including facility issues.
- Business Continuity (BC) - proactive:
 - The ability for companies to make high data availability a reality by eliminating any unexpected and /or planned outages – usually not including loss of the primary facility

Disaster Avoidance



Top 10 Rules for Disaster Planning

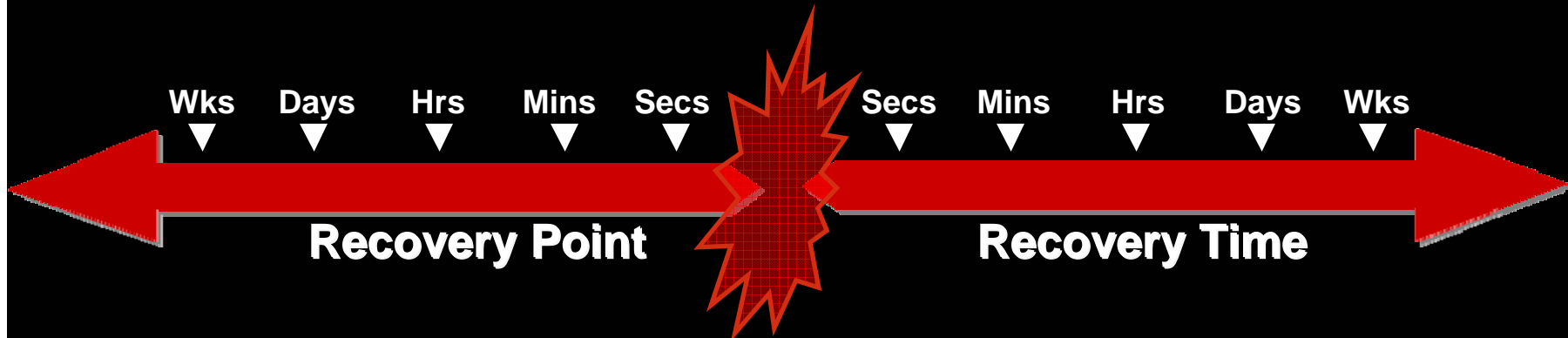
1. Articulate the need in financial terms
2. Use hard data to create a risk profile
3. Identify the Critical Resources
4. Think beyond the data center
5. Eliminate or mitigate single points of failure
6. Assume that everything is going to fail
7. Consider an Active/Active data center strategy
8. Recognize potential vendor weaknesses
9. Keep disaster recovery capability up to date
10. Perform tests on a regular basis

Source: Dell PowerSolutions: Architecting a Blueprint for Disaster Recovery, Feb 2006



Recovery Objectives

Meeting SLA's



- Recovery Point Objective (RPO)
 - How far back in time does data need to be recovered if disaster occurs?
 - How much data are you willing to lose?
- Recovery Time Objective (RTO)
 - How much time will pass after a disaster before operations are online again?
 - How long can you afford to be down?



"Realistic" Target Uptime

Downtime Defined

# of 9's	Percentage	Downtime per Year
1	9%	331 Days 5 Hours 45 Minutes 35 Seconds
2	99%	3 Days 15 Hours 21 Minutes 36 Seconds
3	99.9%	8 Hours 44 Minutes 9 Seconds
4	99.99%	52 Minutes 24 Seconds
5	99.999%	5 Minutes 14 Seconds
6	99.9999%	31 Seconds

Lost revenue based on \$200,000 revenue/day

# of 9's	Percentage	Downtime per Year
1	9%	\$66,248,000.00
2	99%	\$728,000.00
3	99.9%	\$72,800.00
4	99.99%	\$7,280.00
5	99.999%	\$728.00
6	99.9999%	\$72.80



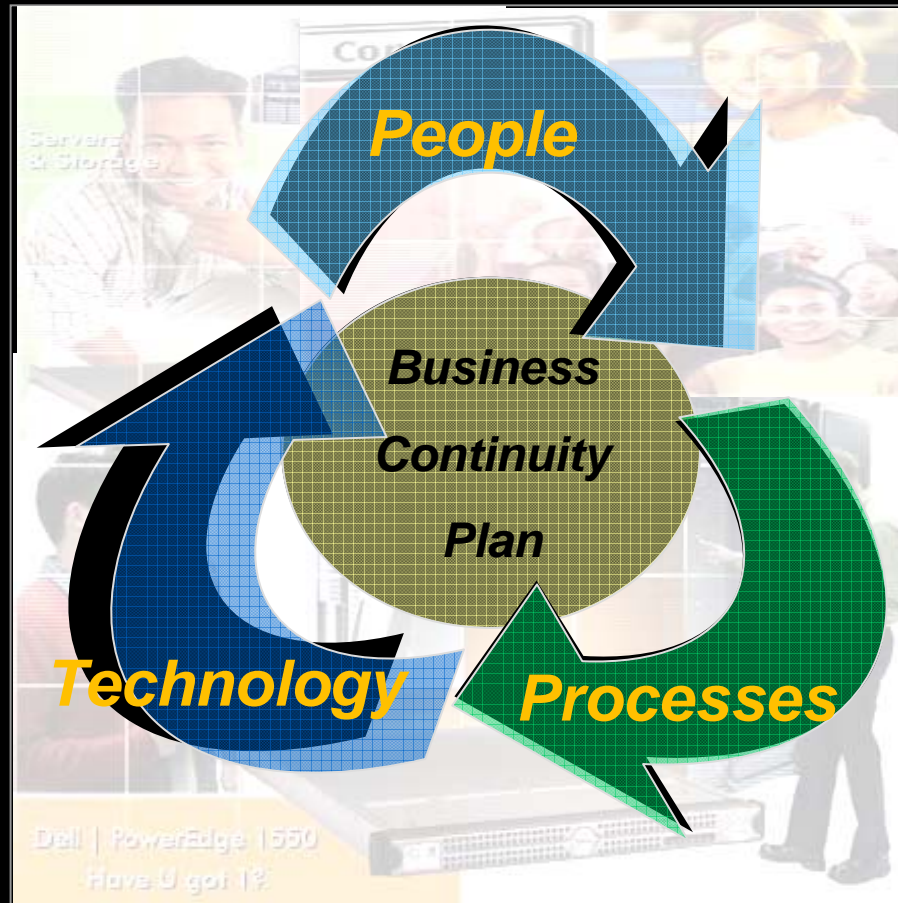
The Plan

Identifies critical people, processes and technologies

Focuses on protecting, maintaining and recovering from planned and unplanned events

Balances vulnerabilities, risks and costs with operational needs when developing requirements

Must be tested and maintained on a regular basis



The Causes of Downtime



Operator error

Examples: unskilled operation, guessing, accidental file deletion



Component failures

Examples: memory, fans, disk drives, power, boards, controllers



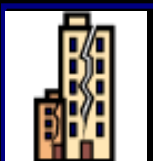
Software failures

Examples: bugs, driver hangs, OS hangs, viruses, file corruption



Planned downtime

Examples: firmware or software upgrades, server reboots



Building disaster

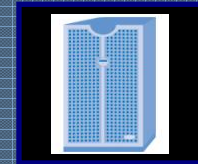
Examples: fire, storms, explosions, collapse, localized disasters



Metropolitan disaster

Examples: earthquake, hurricanes, floods, natural disasters

Vulnerabilities



PLATFORM



DATA



APPLICATION

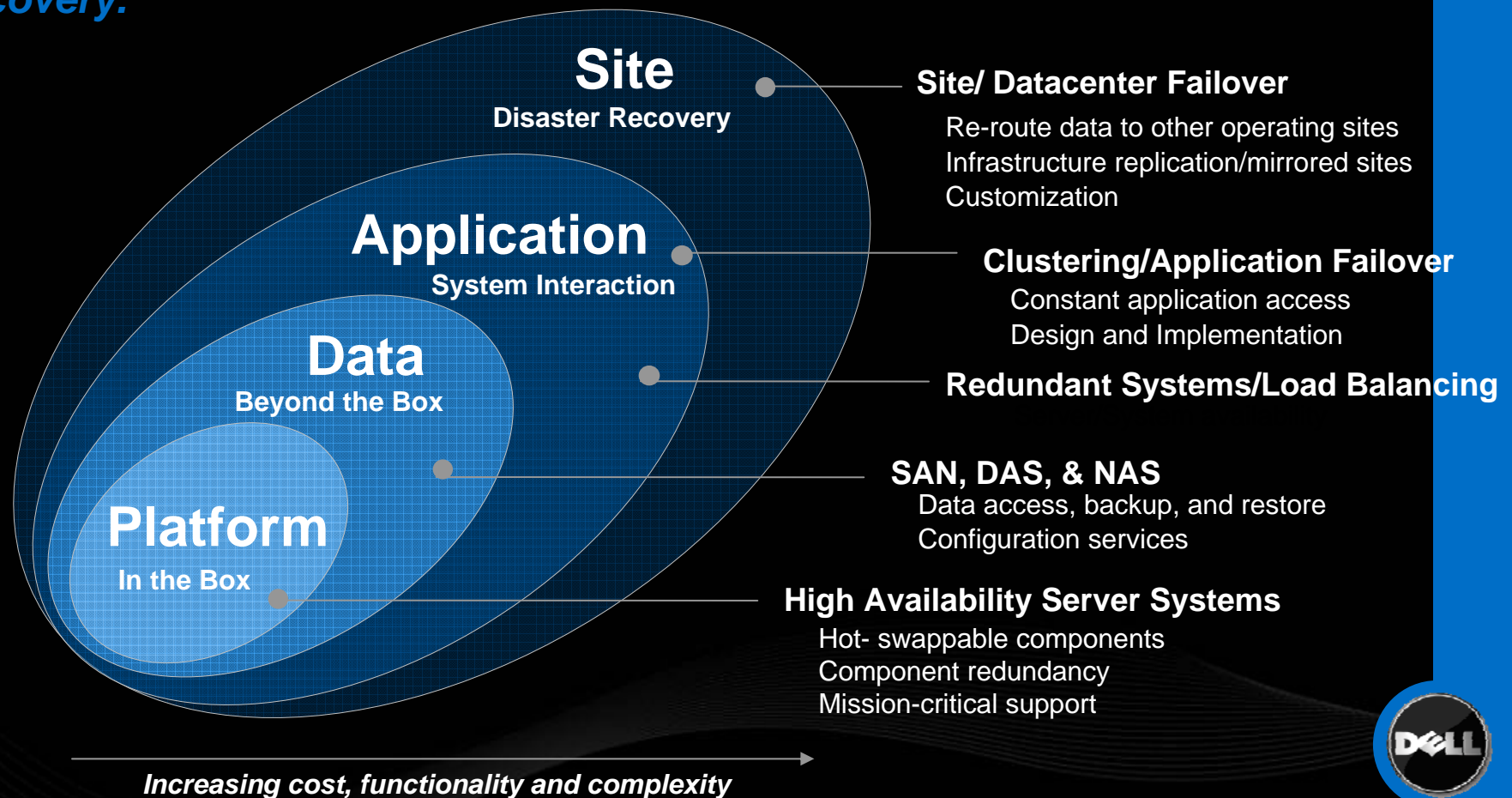


SITE



Availability Continuum

Ensuring access to your data requires eliminating risks that might cause downtime. Availability exists across many levels with each layer in the availability continuum providing additional levels of fault tolerance and/or recovery.



Do you have a Business Continuity / DR Plan?

Evaluation Criteria

1. Do you have a written plan?
2. Is it up to date?
3. Do you test it?
4. Do you test it without the people who wrote it present or participating?

Do it from the Documentation

If you can't do it from the documentation, you will not meet your Recovery Time Objectives in a real disaster!



Slide 9

DCC1

i like this slide. for even more impact, i would change the bottom line to

... you will not meet your recovery time objectives in a real disaster (or real situation)

you might want to include RTO and RPO definitions before this slide - or put a glossary at the end with all of them

Dell Computer Corporation, 9/13/2005

Factors Inhibiting Recovery

Vaulted tapes

Legacy hardware

Backups

Regular Audits

User Connectivity

Documentation

Data on personal systems

Application Software

- take time to retrieve
- often forgotten
- not readily available
- not performed
- not part of the plan
- resides in someone's head
- not backed up
- No copies of Oracle, Exchange, etc vaulted



Disaster Recovery & Business Continuity

Disaster Avoidance



Technologies

Complete Data Protection Overview

Solutions	RPO	RTO	Enabling Technologies
Synchronous-Mirroring, Replication	Zero	Seconds	SRDF, MirrorView/S, EMC Recoverpoint (CDP)
BCV's (clones)	Sec-Hrs	Minutes	SnapView, Microsoft VSS/VDI, EQL Volume Cloning
Snapshots (PITC)	Sec-Hrs	Minutes	SnapView, Microsoft VSS/VDI, ASM, EQL SnapShot, DPM
Asynchronous Replication	Min-Hrs	Min-Hrs	SRDF/A, Mirrorview/A, SanCopy, Open Replicator, EQL Auto Replication, Replistor, Doubletake, CommVault Galaxy, Symantec, DPM
Backup to Disk (B2D)	Hrs-Days	Hrs-Days	EMC Disk Library (EDL), EMC Networker, Quantum, CommVault Galaxy, Symantec Backup Exec, DPM
Improved Tape Technologies	Hrs-Wks	Hrs-Wks	Faster tape drives, Larger/faster Tape Libraries, Faster interfaces

Higher Service Levels

Decreased Recovery Times

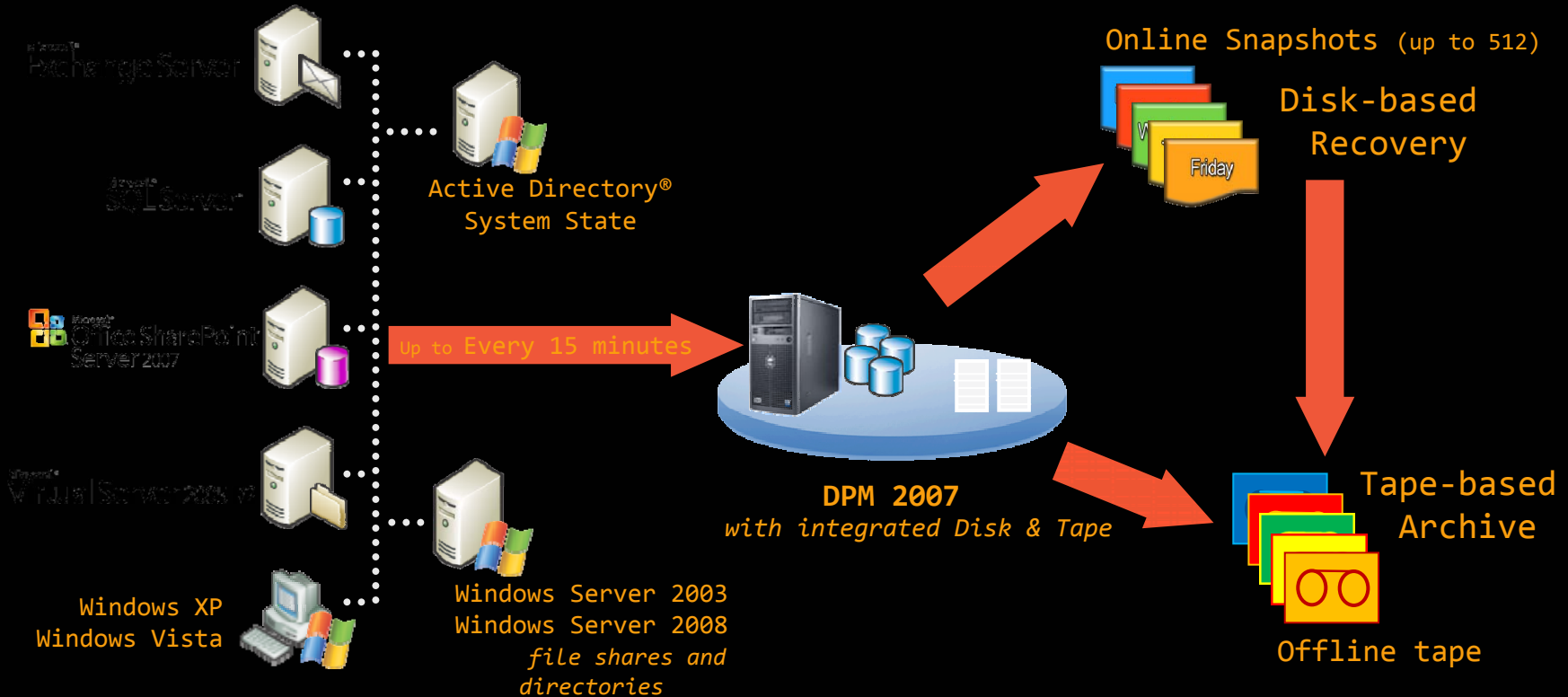


What is Continuous Data Protection (CDP)?

- A new class of disk-based, data protection technology
- Provides immediate access to data at infinitely granular points-in-time
 - Data is captured whenever **any** change is made
 - Recovery points are available for every instant in time
- Quickly recover the most recent copy of the affected data or application
- Most valuable where data changes often, the amount of stored data is large, or where lost or damaged data presents a significant business risk



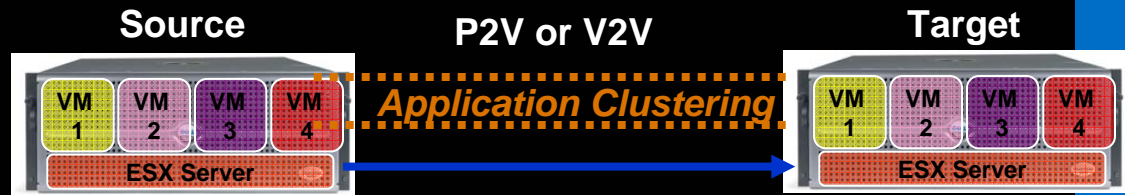
Data Protection Manager



Recovery Time Technologies

Native Application Clustering

- Native Failover with h/w independence
- Software: SQL2005, Citrix, Notes



Vendors Clustering Application

- LAN/WAN Clustering with Replication
- SAN/Storage independent
- Software: NSI DoubleTake, Veritas VCS



Native OS Clustering

- Fast Failover, Application Aware
- Requires SAN and dedicated h/w
- Software: MSCS, NCS, RHELClusterSuite



VMware HA Clustering

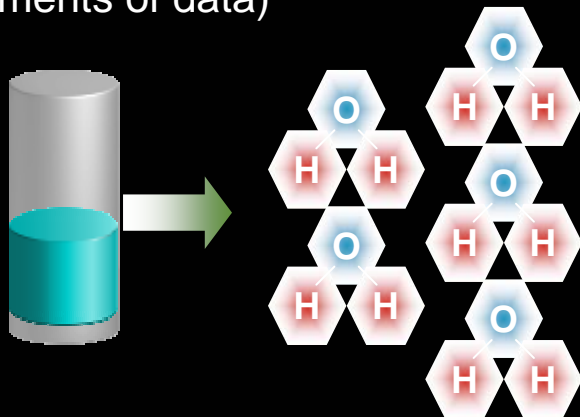
- Clusters any application in V2V on SAN
- Limited data exposure within cache/memory of VM
- Software: VMWare HA



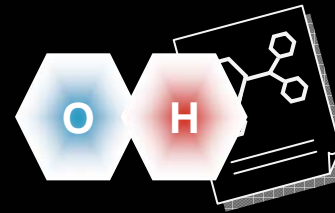
De-Dupe - How it Works

Global Source-based Data De-duplication

① Break data into atom
(sub-file, variable-length
segments of data)



② Send and store
each atom only
once



③ Avamar backup
repository



*...up to 500 times
daily data reduction*

At the source—De-duplication before data is transported across the network

At the target—Assures coordinated de-duplication across sites, servers, and over time

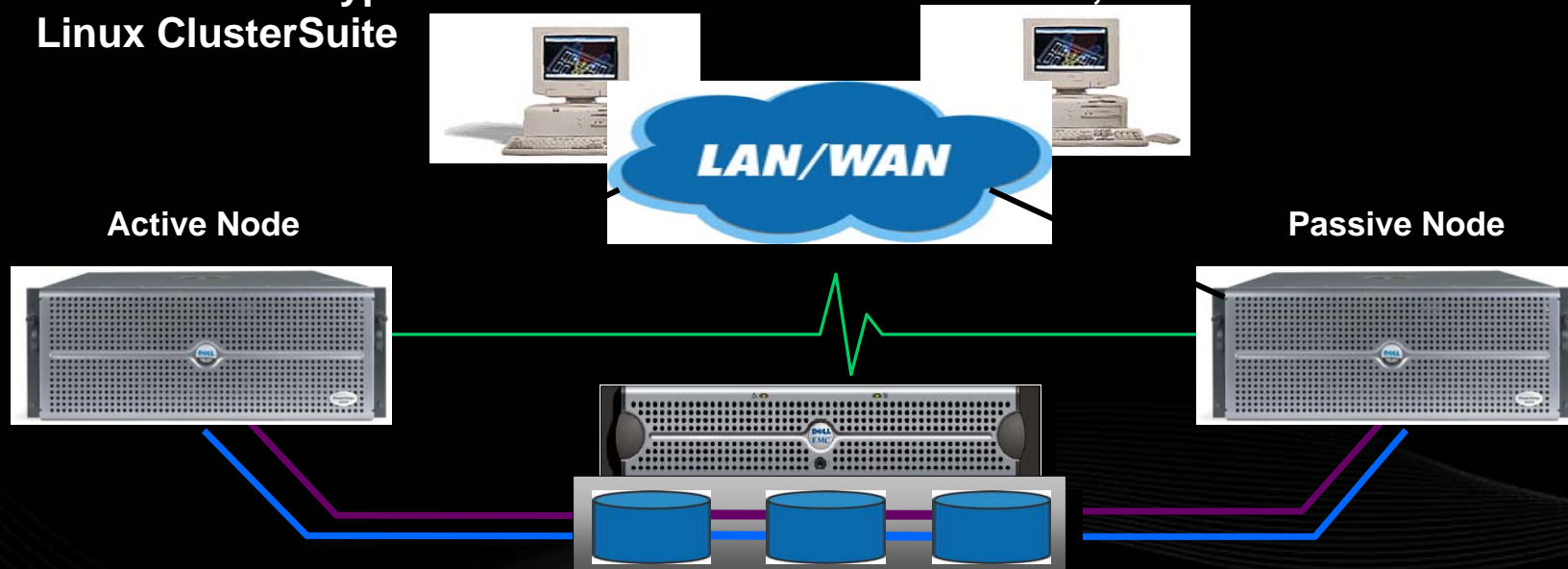
Granular—Small, variable-length sub-file segments guarantee most effective de-duplication



High Availability with MSCS - Shared Nothing Cluster?

What is a Shared Nothing Cluster Model?

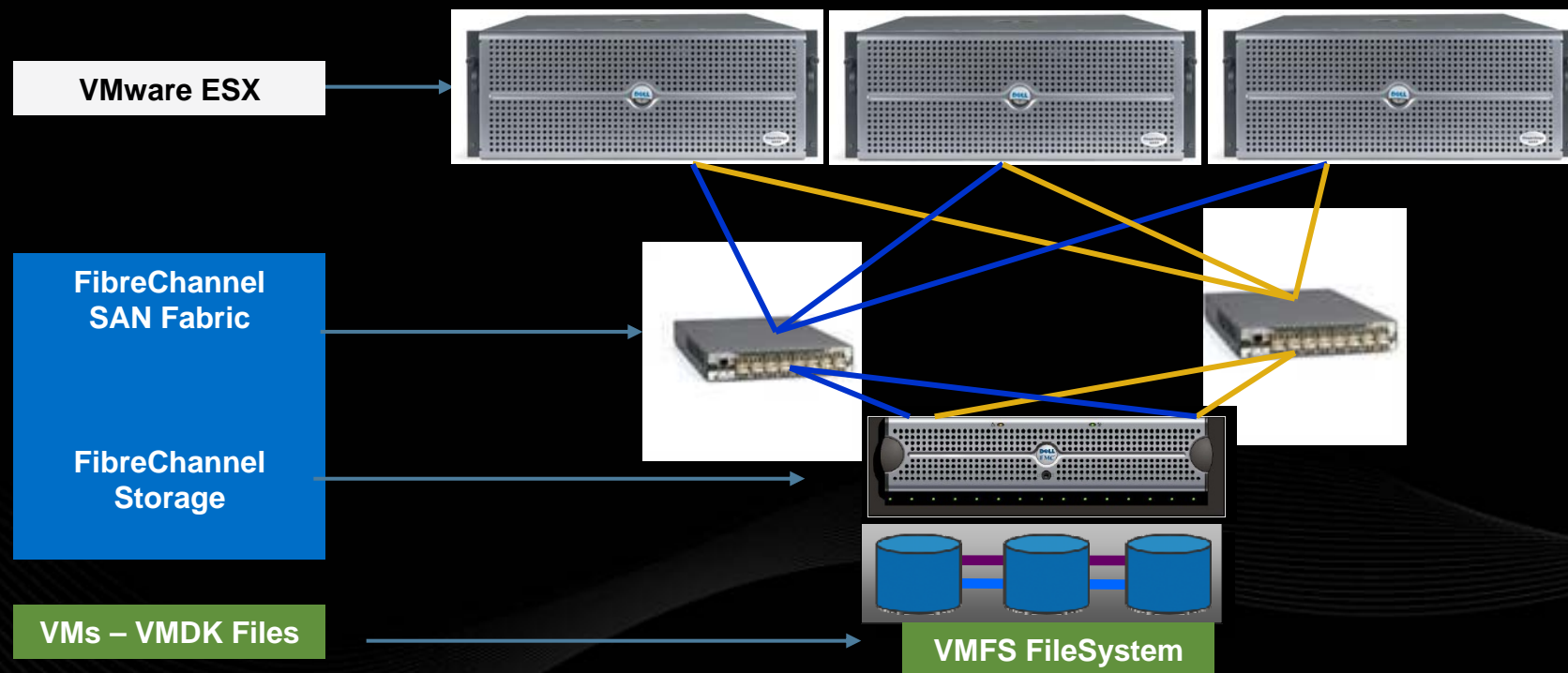
- A “Shared Nothing” architecture is based upon the premise that nodes within the cluster own the resources that they are responsible for.
- Other nodes in the cluster cannot mount the same volumes simultaneously.
- Cluster software controls which server has access to each disk and prevents both from accidentally gaining access.
- Cluster arbitration done using Quorum and Heartbeats
- Most common type of Cluster is MSCS and VCS. Also, Novell Cluster Services, Linux ClusterSuite



VMware HA – Shared Everything Cluster?

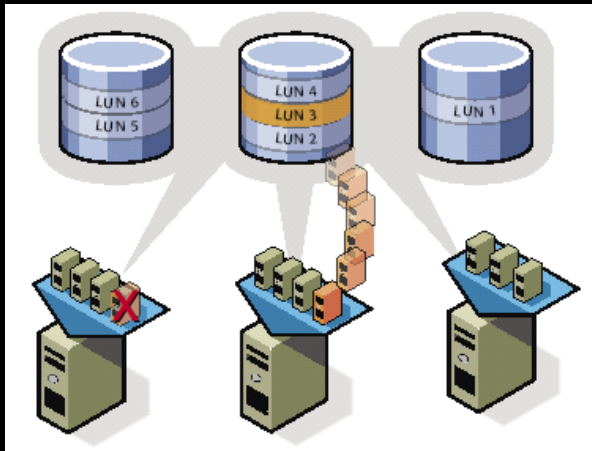
What is a Shared Everything Cluster Model?

- A group of machines that share simultaneous access to a logical resource - LUN
- All nodes within the model can read and write to file and objects that are shared between the systems
- VMFS File System controls Read/Write access to the individual VMs



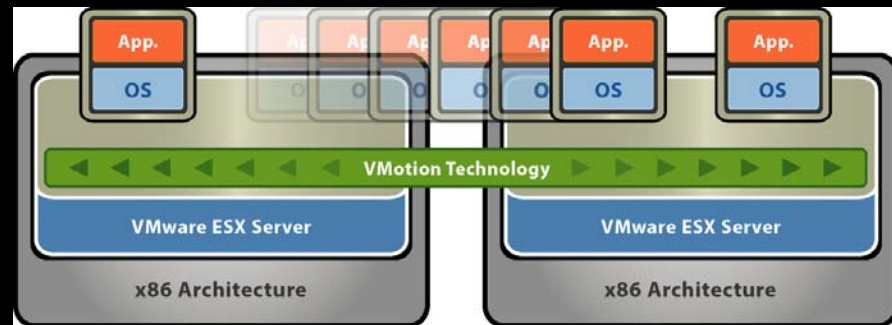
Benefits of Virtualization

Recovery is easier with virtual machines.



- VMs can be restarted on a different physical server
- Downtime limited to VM booting
- Virtual Machines are simply files – easily handled by your IT staff
- Oversubscribe recovery machines to conserve hardware

High availability features not found in physical machines.

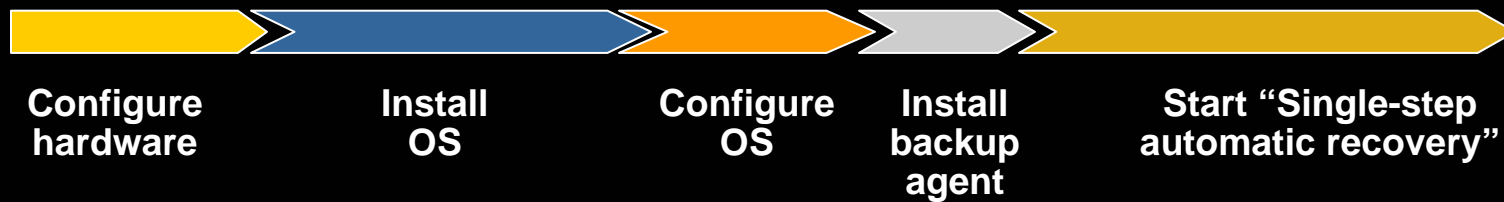
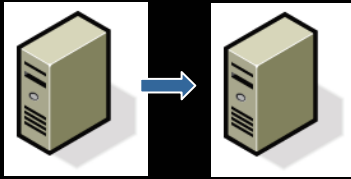


- Eliminate planned downtime with VMotion and Distributed Resource Scheduler (DRS)
- Lower cost and complexity of high availability with VMware HA
- Simplify backup operations with Consolidated Backup

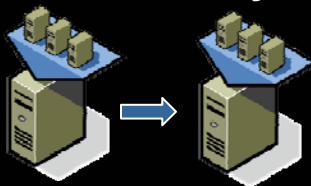


Example Comparison of Recovery Steps

Physical to Physical Recovery



Virtual to Virtual Recovery



Customer Example:

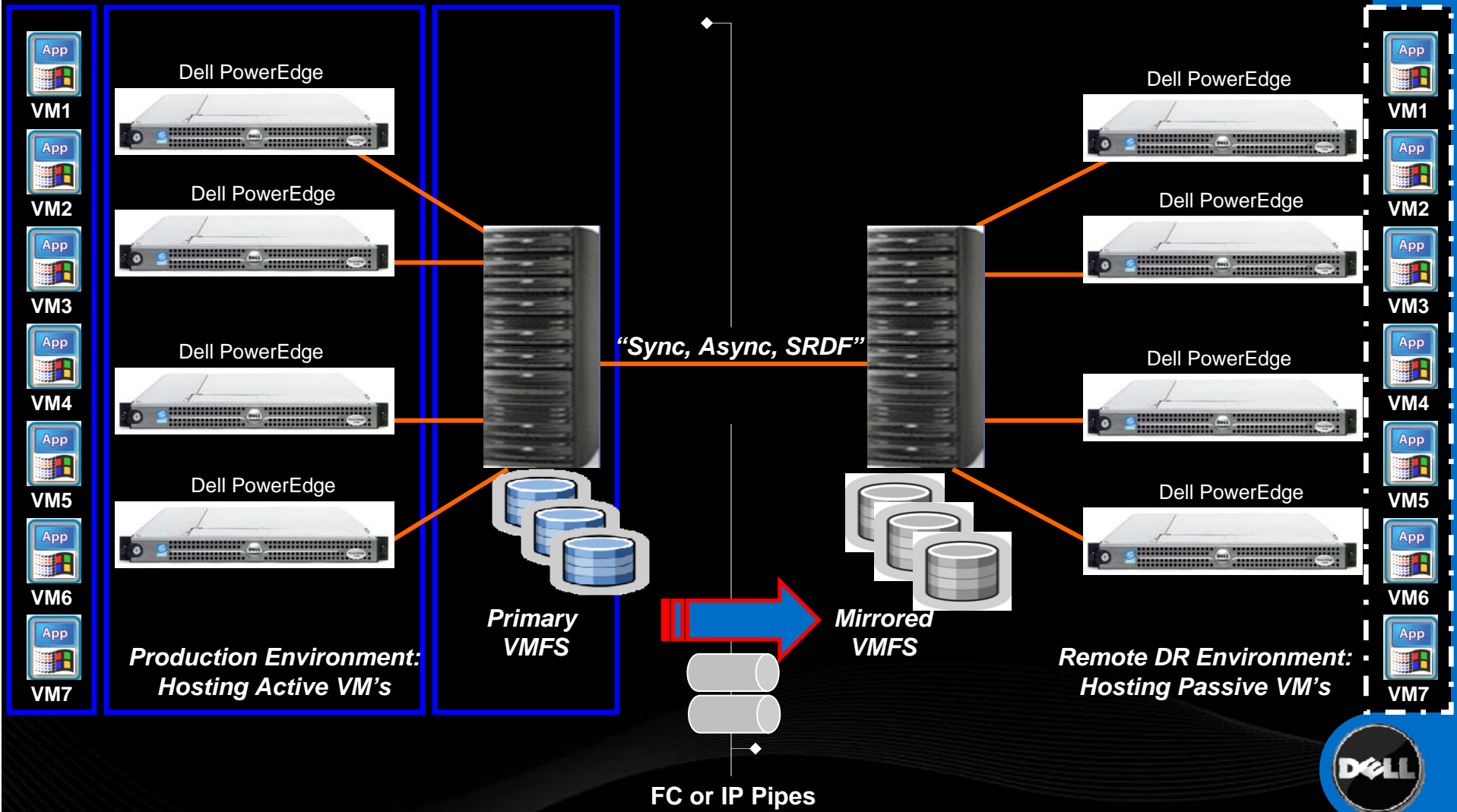
- 40+ hours for physical to physical recovery
- < 4 hours for virtual to virtual recovery



ESX Server - Remote DR

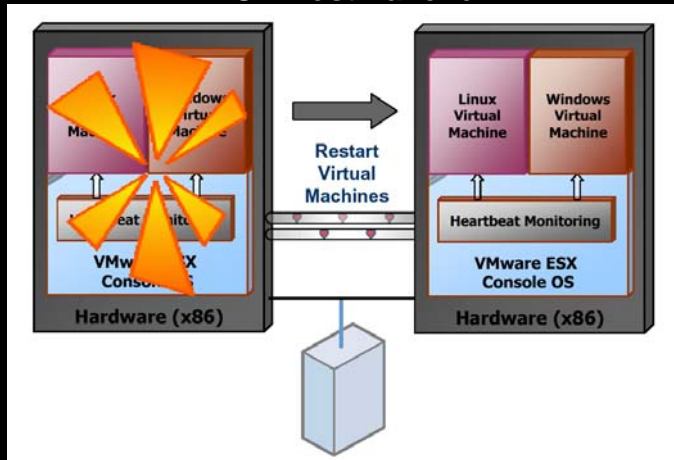
Primary Datacenter "Active"

Secondary Datacenter "Passive"



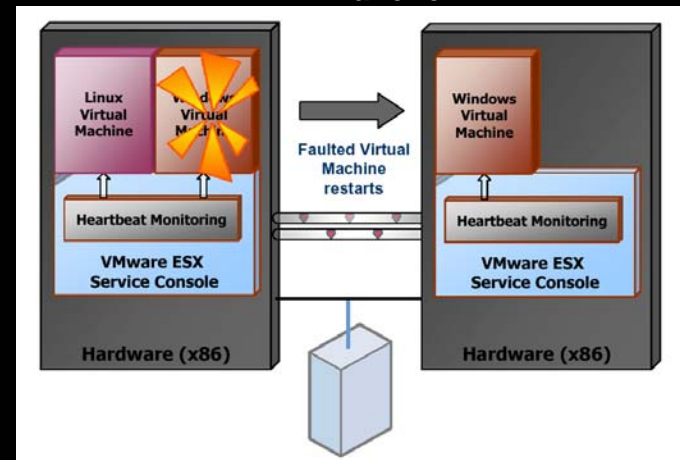
Geographic Clustering with VMware and VCS

ESX Host Failover

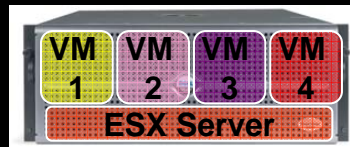


Or

VM Failover



VMware ESX with VCS + MV/SRDF Agent

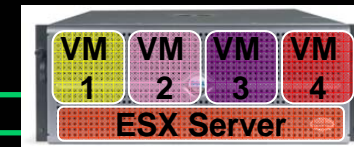


Storage Area Network

Primary Site

Continuity / DR - Site

VMware ESX with VCS + MV/SRDF Agent



Storage Area Network

MV Sync or SRDF





Disaster Recovery & Business Continuity



Dell IT Best Practices

Dell IT Storage Overview

Global Stats

- One of the Largest EMC Control Center Environments
- 2nd Largest Interconnected Brocade SAN in North America
- In the Top 5 Largest Interconnected Brocade SAN's in the World
- 15.8 Petabytes
- 350+ SAN Switches
- 20,000+ FC Ports
- 50,000+ SAN Drives
- 1200+ Provisioning Requests/Yr

Symmetrix (Tier1)

2 EMC Symmetrix 8xxx Arrays
17 EMC DMX-1000/2000/3000 Arrays
10 EMC DMX-3 Arrays

CLARiiON (Tier 2/3)

28 Dell|EMC FC 4700 Arrays
23 Dell|EMC CX600 Arrays
54 Dell|EMC CX700 Arrays
8 Dell|EMC CX3 Arrays

NAS (Network Attached Storage)

7 EMC NS704g
2 EMC NS704i
3 EMC NSX

Backup/Recovery

10 EMC EDL's (Clariion Disk Library)
7 Quantum i2K
14 Legacy Tape Libraries

CAS (Content Addressed Storage)

9 EMC Centera

SAN Fabrics

3 Redundant Core-Edge (Production & DR DCs)
1 Redundant Core-Edge (Lab)



Disaster Recovery Definition

What is Disaster Recovery

An I/T continuity plan based on the critical need for managing people, processes and the recovery of critical applications and hardware, during and after a catastrophic event or disaster



Disaster Recovery & Business Continuity

Hardened Data Centers?

Where is My Risk?

Do I need Continuous Operations?

What won't work?

What's most important?

Leadership

Keeping it Evergreen

What's the Cost?

Invisible Failover?

Is everyone in the Loop?

What about that "extra" capacity?

Build it in, Don't bolt it on

Will My Systems Failover?

DELL

Duplication Across The Datacenters

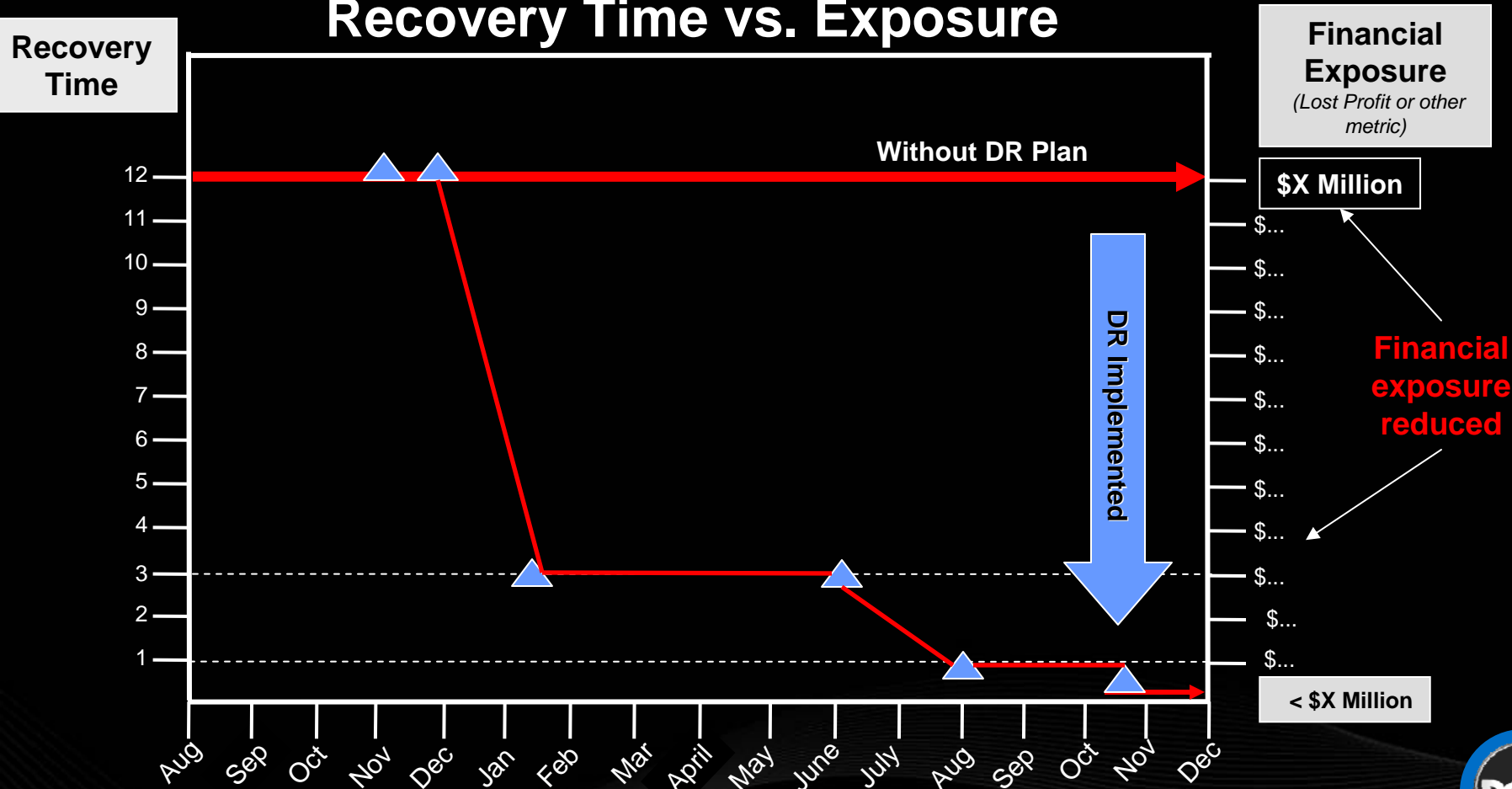


Redundant dark fiber network paths
Redundant application hardware
Application Data Redundancy
Server Traffic Load Balancing



Link to Cost & Impact of Potential Disaster

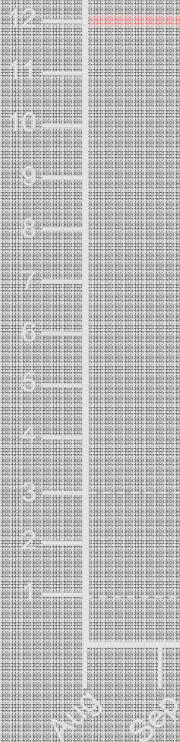
Recovery Time vs. Exposure



Link to Cost & Impact of Potential Disaster

Recovery Time vs. Exposure

Recovery Time

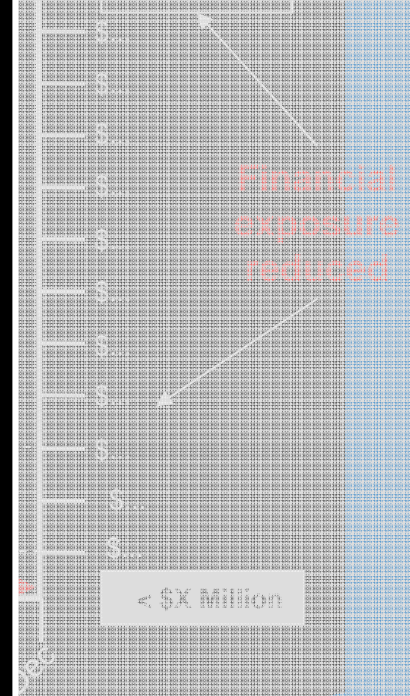


Highlight Financial Benefits

- Estimate financial exposure over the recovery time for loss of each key facility
- Determine best effort recovery time given level of DR capability
- Assess impact of program milestones...
 - Additional Data Center is operational
 - Hardware is ordered
 - Hardware is installed
 - Applications are distributed & Data is replicated
- DR implementation starts delivering value long before all capabilities are fully installed & tested

Financial Exposure
(Lost Profit or other metric)

\$X Million



< \$X Million



Where's Your Risk?

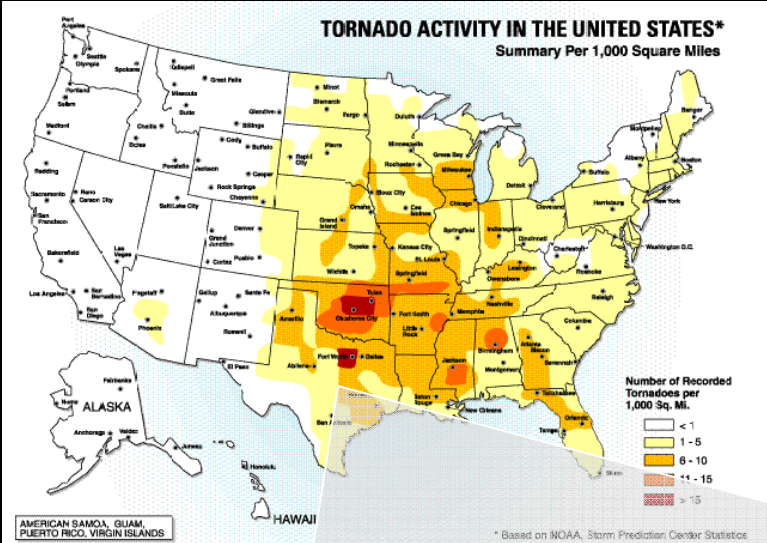


Figure 1.1 The number of tornadoes recorded per 1,000 square miles



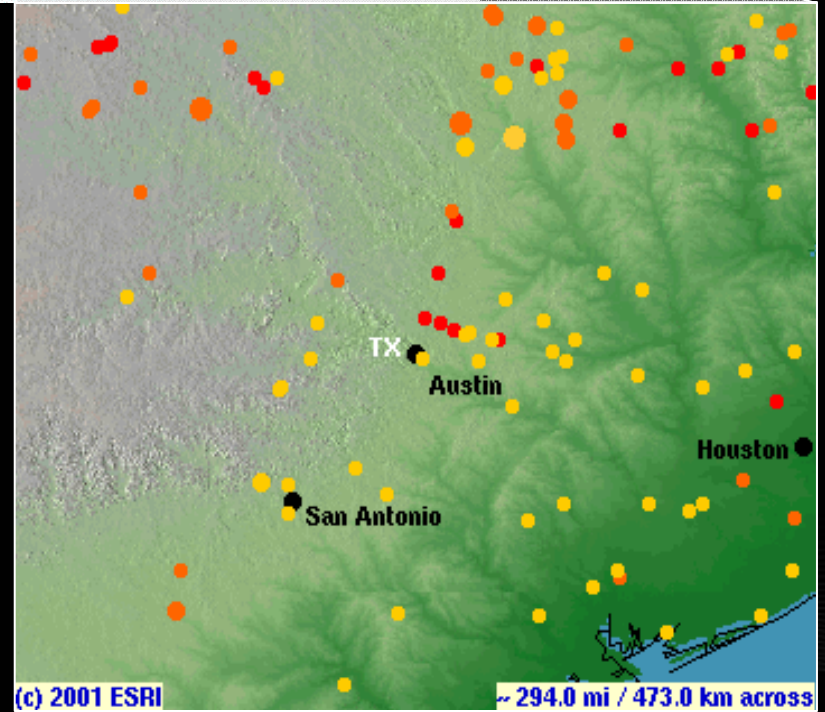
US HISTORIC TORNADOES

Fujita

- 6+
- 5
- 4
- 3

Date

- After 1980
- 1970-1980
- Before 1970



Where's Your Risk?

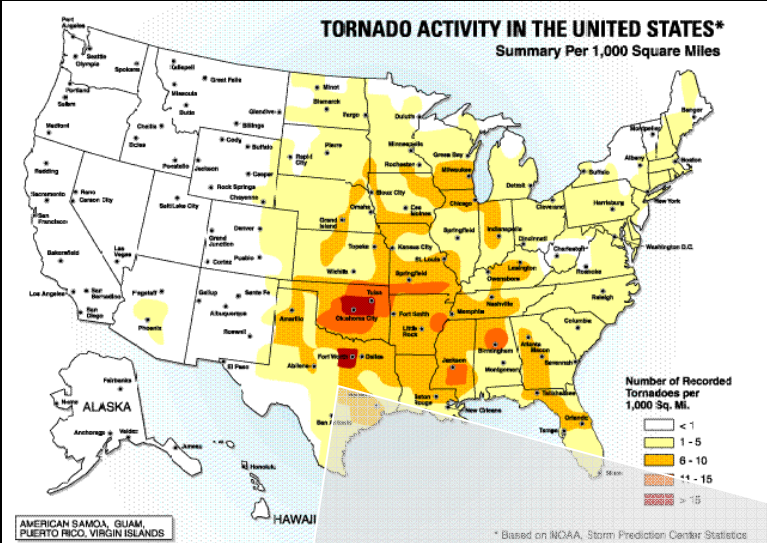


Figure I.1 The number of tornadoes recorded per 1,000 square miles

Top 10 Risks

1. Fire
2. Thunderstorms
3. Utility Interruptions
4. Telecommunications Interruptions
5. Flood or Surface Water
6. Virus
7. Heavy Rain or Snow
8. Extreme Cold or Freezing Precip
9. Water or Liquid Spill or Release
10. Denial of Service Attack

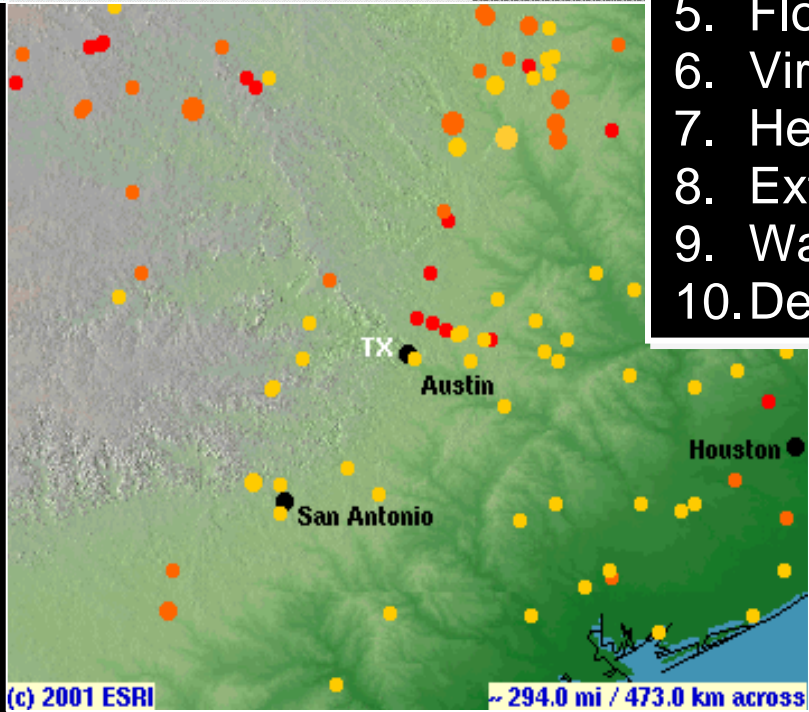
US HISTORIC TORNADOES

Fujita

- 6+
- 5
- 4
- 3

Date

- After 1980
- 1970-1980
- Before 1970



Where's Your Risk?

Top 10 Risks

1. Fire
2. Thunderstorms
3. Utility Interruptions
4. Telecommunications Interruptions
5. Flood or Surface Water
6. Virus
7. Heavy Rain or Snow
8. Extreme Cold or Freezing Precip
9. Water or Liquid Spill or Release
10. Denial of Service Attack

Leverage Your Insurance Carrier

- Expert at risk analysis
- Maintains extensive loss databases
- Motivated to reduce your risk
- Can drive premium reductions

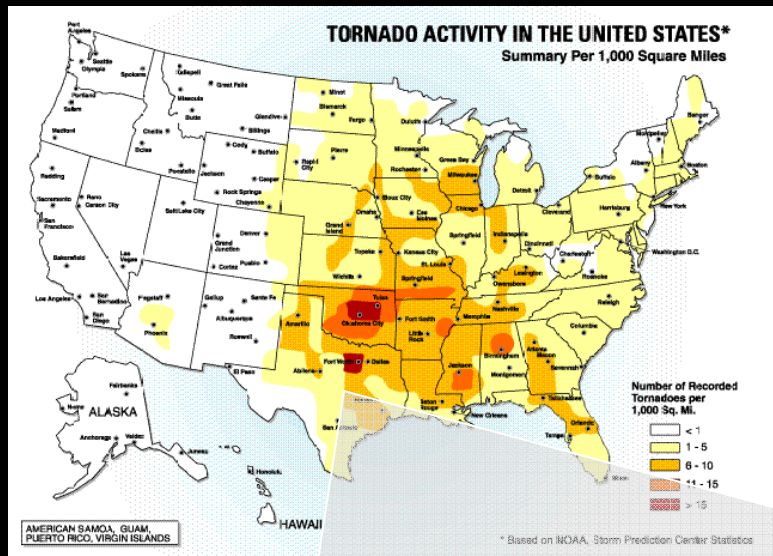


Figure 1.1 The number of tornadoes recorded per 1,000 square miles

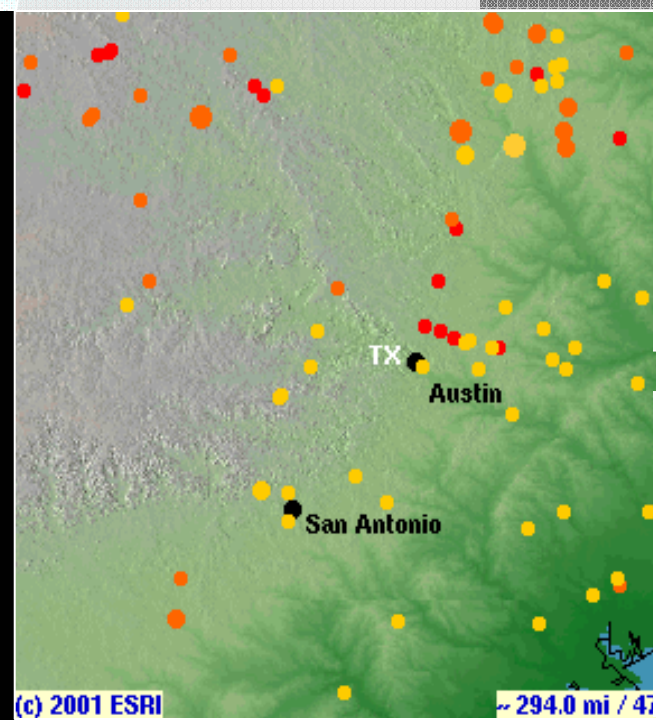


Fujita

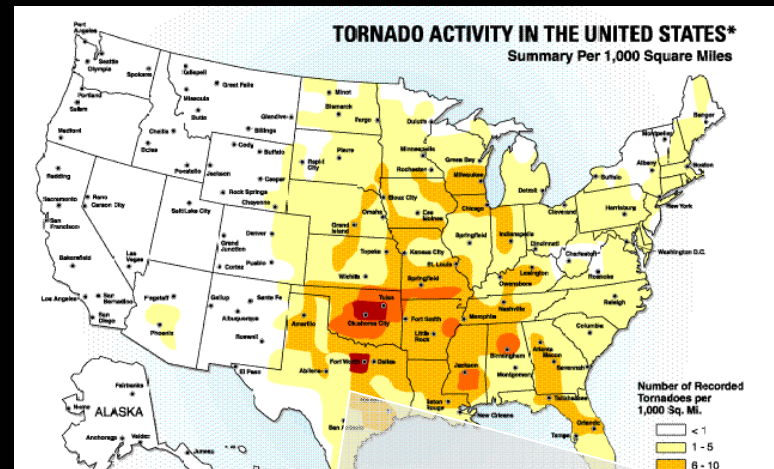
- 6+
- 5
- 4
- 3

Date

- After 1980
- 1970-1980
- Before 1970



Where's Your Risk?



Other Risk Considerations

- Tornado
- Earthquake
- Hurricane/Typhoon
- Terrorist Attack
- Human Error
- Tsunami
- Etc. . . .

*Each Business & Location
will have a unique Risk Profile*

- 1970 - 1980
- Before 1970

(c) 2001 ESRI

~ 294.0 mi / 47

Top 10 Risks

1. Fire
2. Thunderstorms
3. Utility Interruptions
4. Telecommunications Interruptions
5. Flood or Surface Water
6. Virus
7. Heavy Rain or Snow
8. Extreme Cold or Freezing Precip
9. Water or Liquid Spill or Release
10. Denial of Service Attack

Leverage Your Insurance Carrier

- Expert at risk analysis
- Maintains extensive loss databases
- Motivated to reduce your risk
- Can drive premium reductions

Dell's DR Classifications

DR Class	DR Class Description	RTO*
I Business Critical	<i>Any outage immediately impacts the business</i>	1-4 Hrs
II Business Essential	<i>An extended outage (i.e., > 48 hours) impacts the business</i>	48 Hrs
III Business Support	<i>An extended outage does not impact the business</i>	Best Effort

* Recovery Time Objective

What "impacts the business"?

- Degrades business operations
- Impacts customer experience
- Results in financial loss
- Erodes brand value
- Creates unacceptable liabilities

Business Impact Analysis

1. Define Business Impact in terms relative to your business
2. Relate I/T Resources to Impact of their loss or degradation
3. Assess Applications, Data & Infrastructure
4. Ensure Single Points of Failure are identified & mitigated
5. Include components which support critical resources
6. Link to financial exposure
7. Involve & validate with business owners
8. Make DR Class part of the culture
9. Periodically update

Single Point of Failure (SPOF) Analysis

Conduct analysis of Single Points of Failure (SPOF) in Class I (Business Critical) Systems to ensure Business Continuity

Single Point of Failure (SPOF)

- A point in a system where if a failure occurs, there is no redundancy to compensate for it
- Systems can have more than one “single point of failure”
- One SPOF in a critical component can overshadow well engineered redundancies & resilience in the rest of the system
- Removal of all SPOFs usually not cost effective
- Leverage Failure Mode & Effect Analysis (FMEA) & other tools

I/T Resources to be Analyzed

Client Systems

Application Software

Middleware

Up Stream Systems

Data

Shared Services

Network – Facility

Network – Long-Haul

Network – Campus

Servers

Storage

Environmental

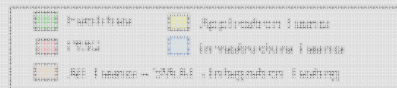
Power

Data Center Facility



Build the Team . . . Manage the Complexity

Roadmap - Disaster Recovery Phase 1



Grey box = Completed (before end of FY02 Project)



- Application teams
- Data Management
- I/T Operations & Engineering
- Networking & Telecom
- Facilities
- Business Customers
- Business Continuity Program
- Our Program Approach...
 - 20,000+ Tasks
 - 2 years
 - Dedicated PMO driving extended virtual teams
 - Phased Program
 - Earned Value & Scorecarding



Disaster Recovery Testing

Scope...

- Business Critical Systems
- Key systems of critical vendors
- Paper review on some

Strategy...

- Cross-Functional Planning
- Limited Business Disruption
- Not a one-time event

Objectives...

- Validate recovery procedures
- Demonstrate recoverability SLA
- Identify recoverability problems
- Test end-to-end failover integration

Metrics...

- Recovery time
- Procedural Errors
- Data Integrity
- Functional Availability

Make Testing a Regular Cycle...

- Test some Apps each Quarterly
- Test all Business Critical App Annually
- Each Test requires planning, staging, execution & analysis

Q1

Q2

Q3

Q4



Disaster Recovery Testing

Scope...

- Business Critical Systems
- Key systems of critical vendors
- Paper review on some

Strategy...

- Cross-Functional Planning
- Limited Business Disruption
- Not a one-time event

Objectives...

- Validate recovery procedures
- Demonstrate recoverability SLA
- Identify recoverability problems
- Test end-to-end failover integration

Metrics...

- Recovery time
- Procedural Errors
- Data Integrity
- Functional Availability

Make Testing a Regular Cycle...

- Test some Apps each Quarter
- Test all Business Critical App Annually
- Each Test requires planning, staging, execution & analysis

Q1

Q2

Q3

Q4



If it hasn't been tested, it doesn't work...



Key Takeaways . . .

Getting It Done . . .

- *Start with Leadership*
- *Integrate with the Business*
- *Assess the Risks*
- *Identify the Critical Resources*
- *Balance Cost & Benefit*
- *Involve the Entire Team*
- *Harden your Data Centers*
- *Go Active-Active*
- *Assume Nothing Will Work*
- *Do a Full Failover*



Key Takeaways . . .

Keeping It Evergreen...

- *Build DR into every Solution*
- *Don't Break into the "Piggy Bank"*
- *Test it . . . Regularly!*

*Make DR part of your Culture
Every Project, Every App, Everyday*



Questions and Answer

To take advantage of complete Business Continuity / Disaster Recovery solutions offered by Dell and EMC. Please contact your Dell Sales representative and Visit us at:

www.dell.com/businesscontinuity

