Enterprise Continuity For Government

Dick Kallmeyer

Sr. Solutions Marketing Manager

dick.kallmeyer@sun.com

Sun microsystems

We make the net work.

Agenda

- Continuity Basics
- Architectures for Continuity

The Issue

“There cannot be a crisis next week. My schedule is already full.”

Henry Kissinger

The Pressures

- Post- 9/11 continuity requirements
- Growing regulatory compliance issues
- Fiduciary, Audit
- Insurance (Basel II)
- Litigation
- Etc....

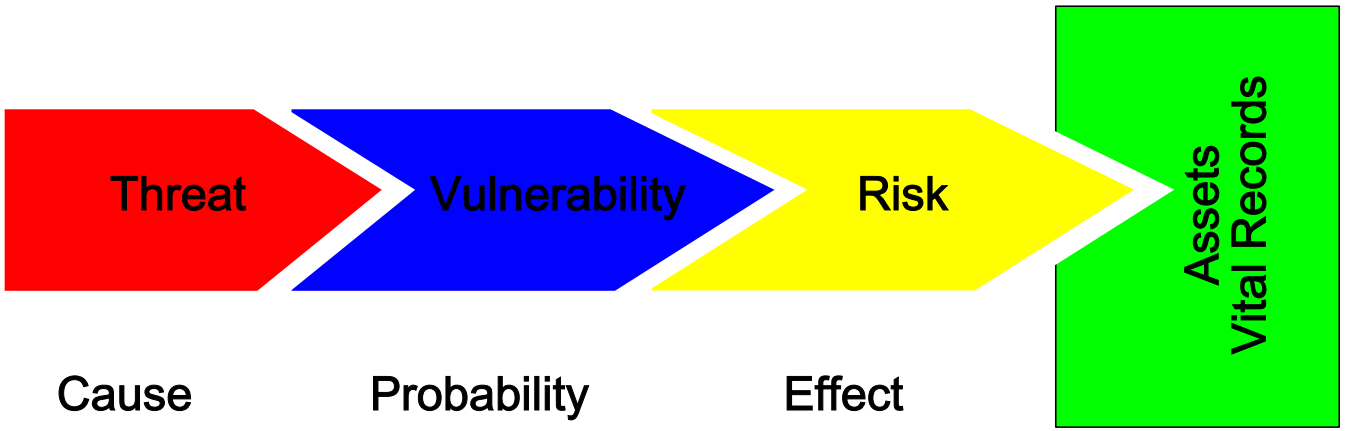
The Impact in the Commercial World

Industry	Lost Revenue Per Hour	Lost Revenue Per Employee Hour
Energy	$2,817,000	$589
Telecomm	$2,066,000	$187
Manufacturing	$1,610,000	$134
Finance	$1,495,000	$1,079
Information Technology	$1,344,000	$184
Insurance	$1,202,000	$370
Retail	$1,107,000	$244
Pharmaceutical	$1,082,000	$167
Chemicals	$704,000	$194
Transport	$668,000	$107
Utilities	$643,000	$142
Health Care	$636,000	$142
Media	$340,432	$119

Some Terminology

- **COOP** – Continuity of Operations
  - Supports the continuance of government functions
- **COG** --- Continuity of Government
  - Addresses the continuance of constitutional governance
- Business Continuity **(BC)** is the business objective that deals with a organization's ability to continue critical functions, in the face of unforeseen events.
- Disaster Recovery **(DR)** refers specific tasks undertaken in the event of a loss by an organization.
- Business Impact Analysis **(BIA)** ***identifies and prioritizes the minimum enterprise business continuity*** **requirements to stay in business at certain levels of disruption.**

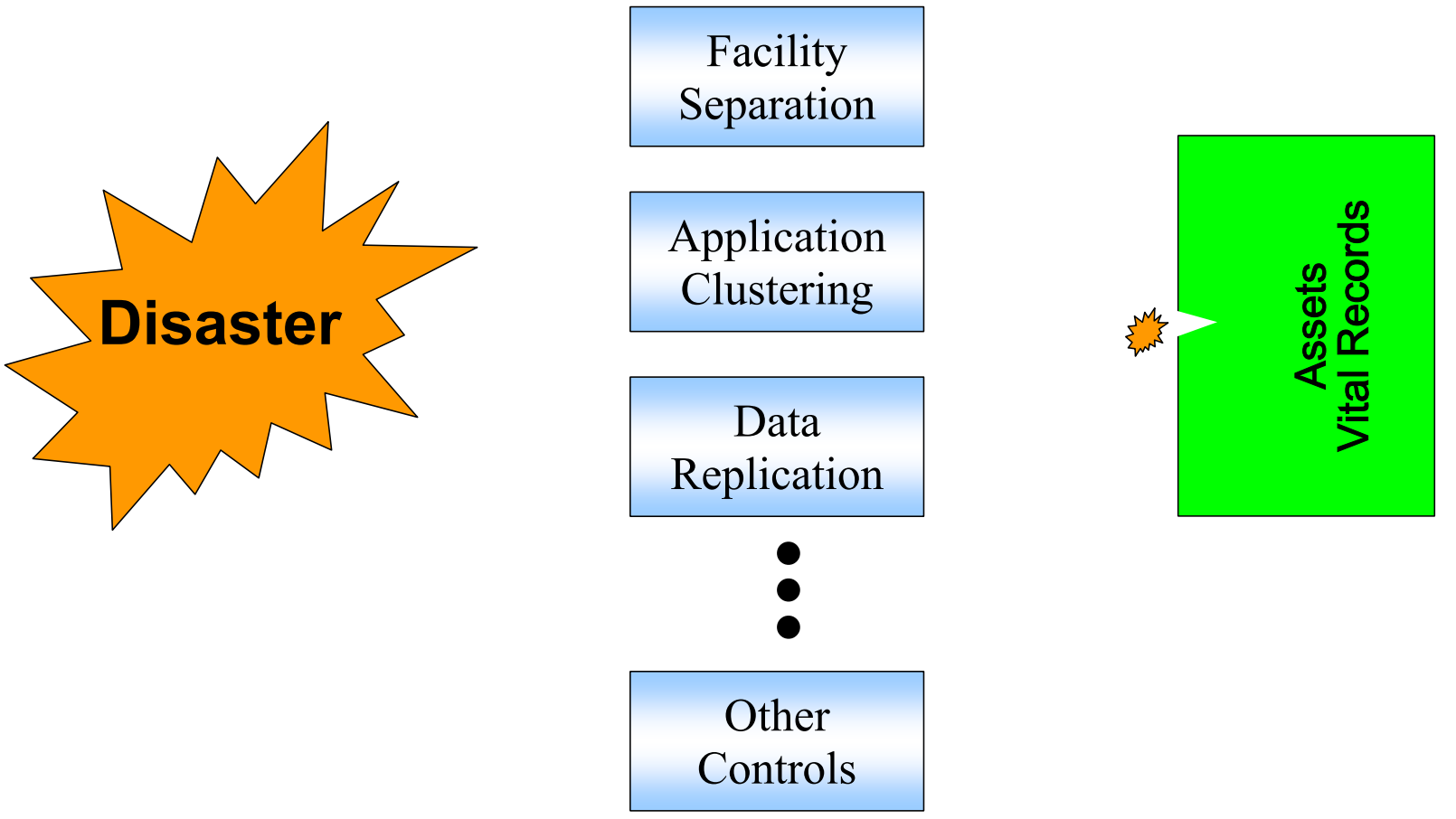
Some Terminology



What is a “Disaster”?

- A Disaster is a sudden unplanned calamitous event causing great damage or loss.
- A Disaster is an event
  - That creates an inability on an organization’s part to provide the critical business functions for some predetermined period of time
  - The period when an organization decides to divert from normal production responses and exercises its disaster recovery plan.
- Similar terms: Organization Interruption, Outage, Catastrophe.

“Controls” Mitigate the Effects of Risk



How Far Offsite?

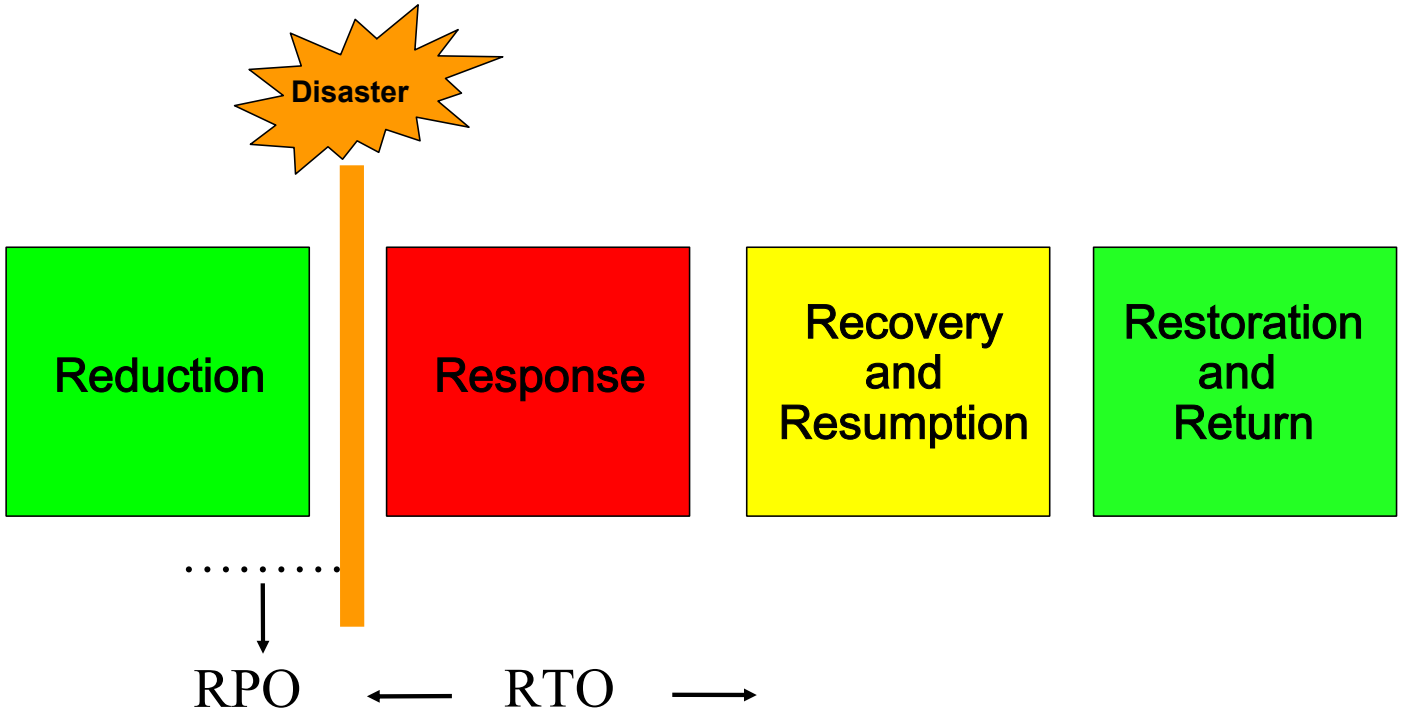
Threat/Risk	Alternate Facility (*Miles*)	Offsite Storage (*Miles*)
Hurricane	105	*84*
Volcano	75	62
Snow/Sleet/Ice	68	50
Earthquake	60	46
Tsunami	51	44
Flood	46	44
Military Installation	44	41
Forest Fire	42	38
Power Grid	31	33
Tornado	29	25
Central Office	28	27
Civilian Airport	26	24

"the new thinking is that a DR site must be within a five-hour drive of the main facility with at least two available routes by car."

Choosing a Location For Your Disaster Recovery Facility, *Disaster Recovery Journal, Winter 2004*

Source: **PreEmpt** Inc for the Association of Contingency Planners (ACP)

The Recovery Process



Reduction: The Planning Phase

The Objectives of a COOP plan should include*:

1. Ensuring the continuous performance of an agency's essential functions or operations during an emergency
2. Protecting essential facilities, equipment, records, and other assets
3. Reducing or mitigating disruptions to operations
4. Reducing loss of life, minimizing damage and losses
5. Achieving a timely and orderly recovery from an emergency and resumption of full service to customers.

** **Federal Preparedness Circular (FPC) 65**, United States Government*

Effective COOP Plan Elements

1. Plans and procedures
2. Essential functions defined
3. Delegations of authority
4. Orders of succession
5. Alternate facilities identified
6. Communications and warning
7. Protection of vital records and databases
8. Testing, training, and exercises
9. COOP implementation
10. Roles and responsibilities
11. Update, distribution, and communication of plan
12. Hazard identification and risk assessment
13. Mitigation and countermeasures
14. Logistics
15. Command and control

Recovery Objectives

Fast Disaster Recovery

RTO: 1 - 4 hours
RPO: 0 – 5 min

Business Continuity

RTO: < 1 hour
RPO: 0 – 5 min

Slow Disaster Recovery

RTO: 1 – 7 days
RPO: 1 – 24 hours

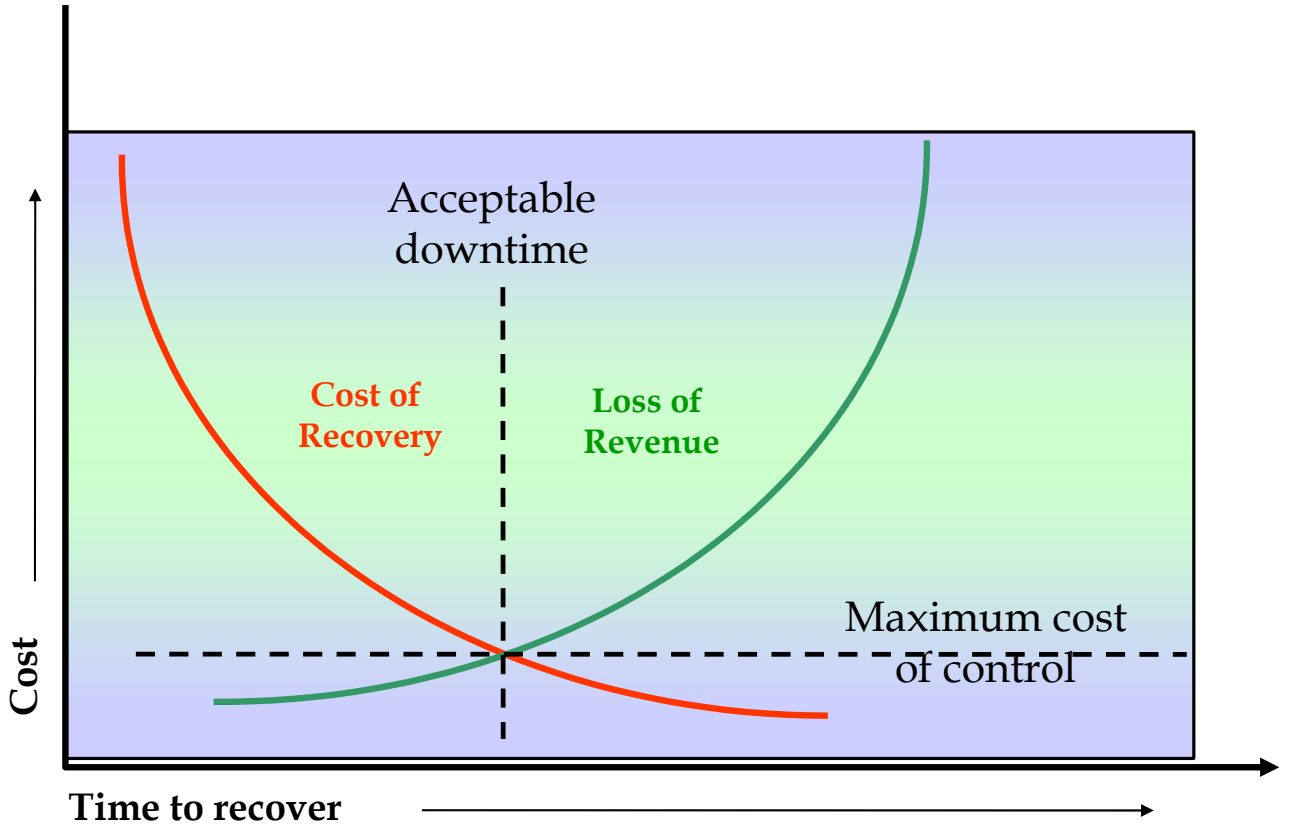
Medium Disaster Recovery

RTO: 1 - 24 hours
RPO: 5 min

Recovery Point Objectives (RPO): The time between the last safe backup and the point of time of the disaster

Recovery Time Objectives (RTO): The time elapsed from when the disaster occurred to the resumption of normal business activities

Optimum Cost of Recovery



Why Continuity Plans Fail (Meta Group)

- Lack of education and awareness of explicit roles and responsibilities
- Lack of testing process/procedures
- Lack of maintenance/updates
- Creation of voluminous and complex plans (resulting in documentation being difficult to maintain and recovery not being staged)
- Building of plans without the confidence of business impact analysis (BIA) data
- Plans do not meet recovery point objectives (RPOs — e.g., data currency) or recovery time objectives (RTOs)

Why Continuity Plans Fail (continued)

- Lack of integration with DR (e.g., data center plans not providing voice/data network, systems, and personnel support for work-area recovery)
- Lack of governance (i.e., who, what, where, and when
- Overinvesting in the recovery of non-essential systems and data
- Not defining a “return to normalcy” timeline
- Treating e-mail and/or telephones as non-mission-critical
- Lack of coordinated communication
- Insufficient work area recovery space

Architecture Solutions for Continuity

Not All Data Is Equal!

- **15% is Mission Critical**
  Data that is used in key processes. Minimum acceptable work levels in the event of a disaster. Data that must be retained for legal reasons.

- **20% is Vital**
  Data that is used in normal processes that represents a substantial investment of company resources that may be difficult if not impossible to recoup. May not be immediately required for a disaster recovery. May be considered company secret.

- **25% is Sensitive**

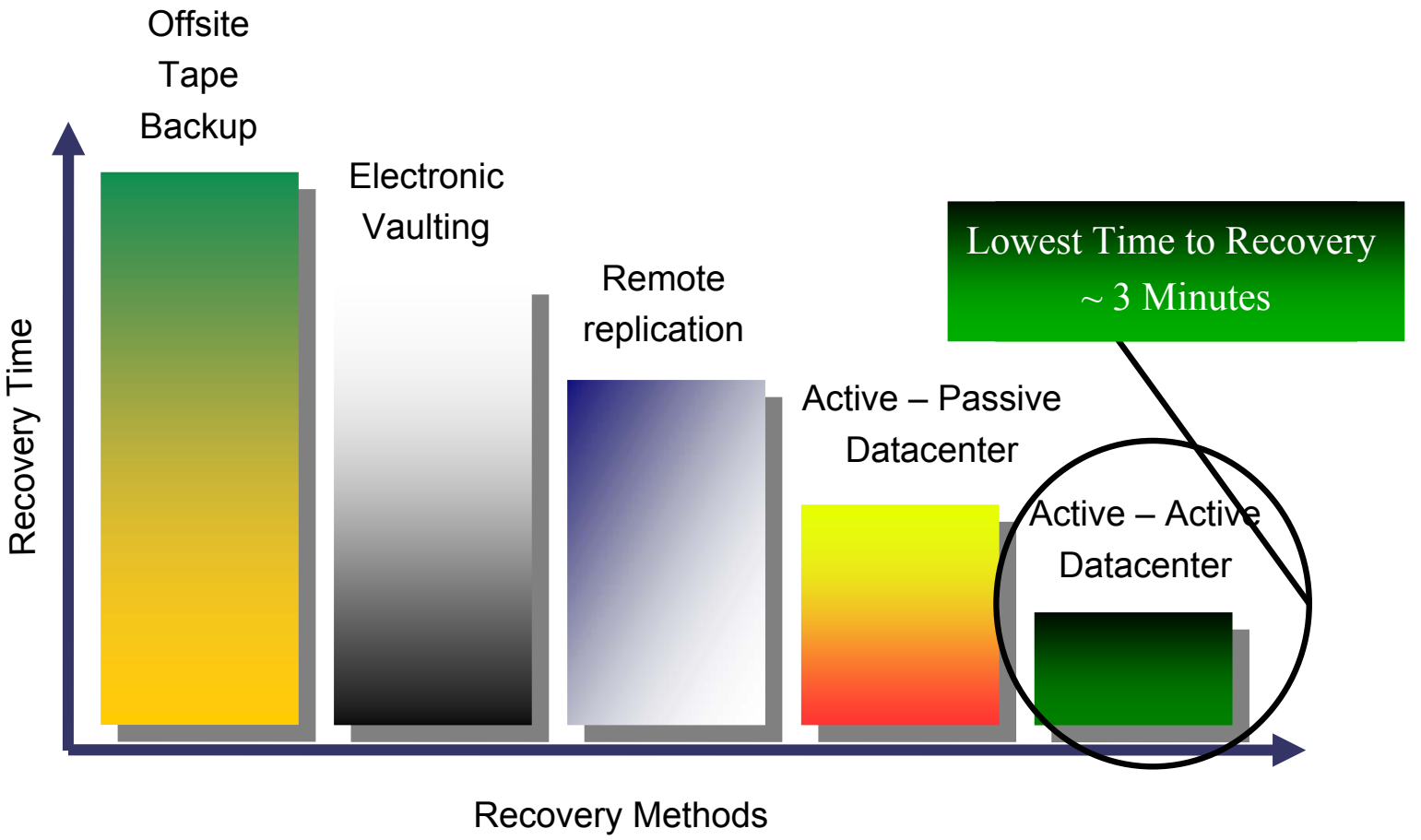
  Data used in normal operations for which there are alternate sources available in case of loss. Data that can be reconstructed fairly easily.

- **40% is Non-Critical**

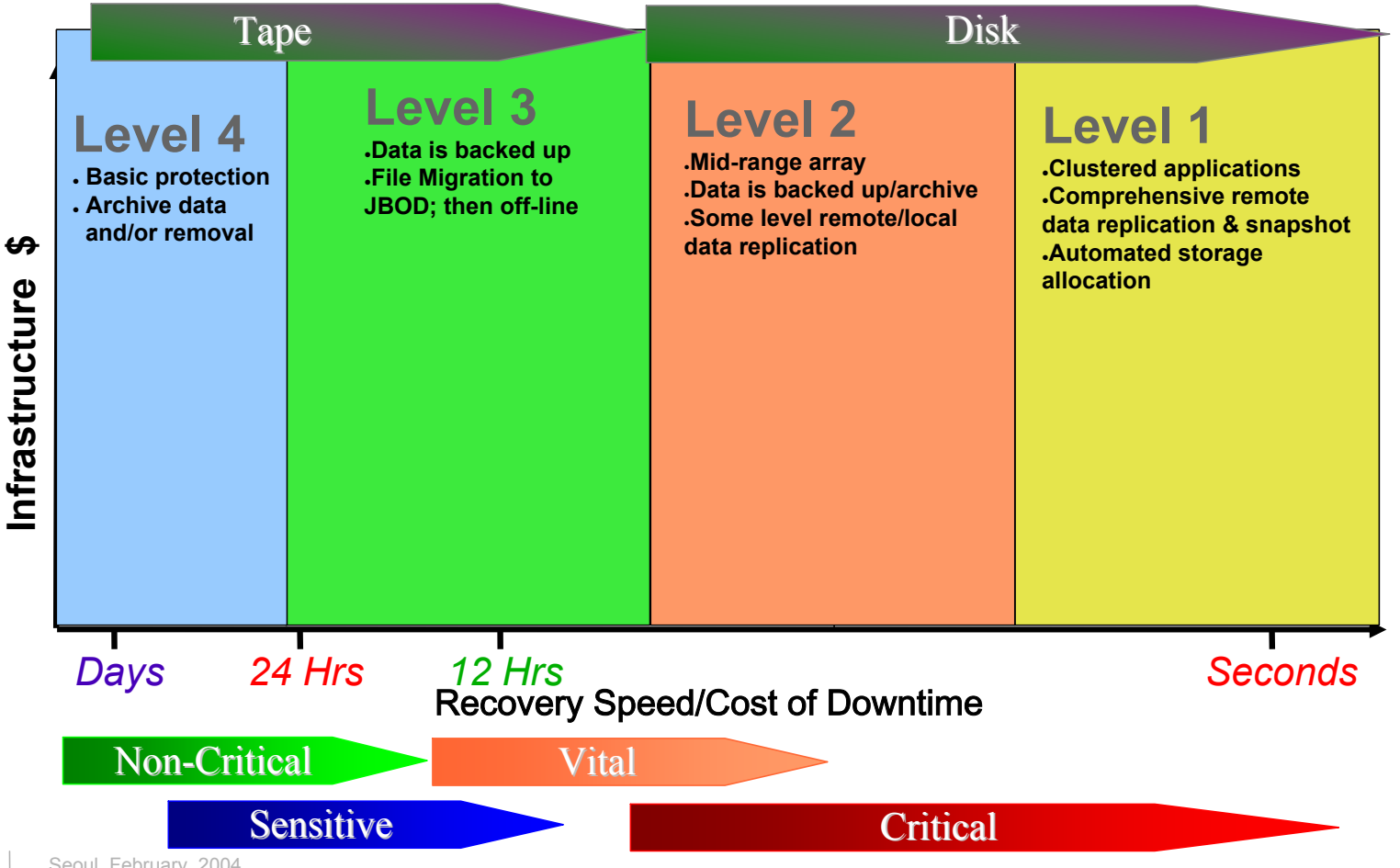
  Data that can be reconstructed easily with minimal cost. Duplicates of existing data that have low security requirements.

Source: Horison Informations Strategies

Which Continuity Strategy?



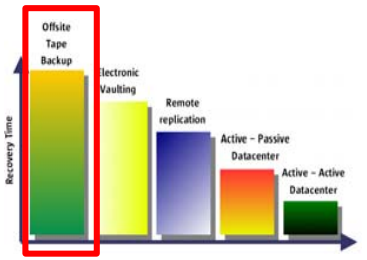
Options for Data and Application Recovery

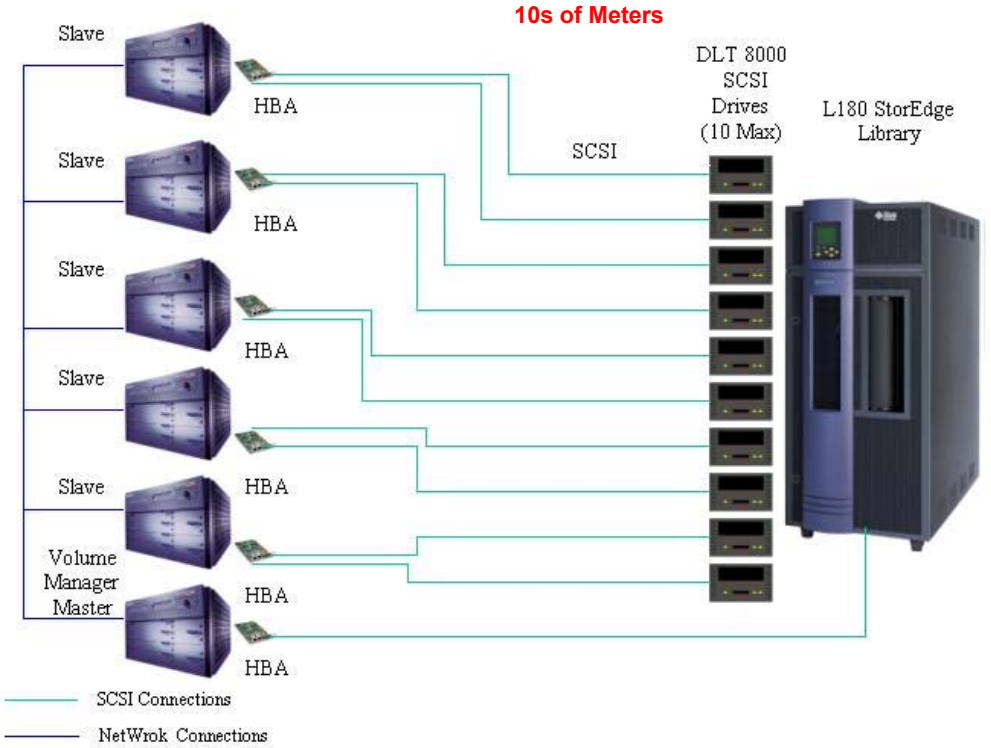


IT Continuity Solutions

- **Logical (Application Based) Data Replication**
  - low bandwidth / high maintenance, relatively cheap
- **Host Software Based Replication**
  - medium bandwidth / medium maintenance
- **Storage Based Replication**
  - high bandwidth / medium maintenance, costly
- **Clustering**
  - high bandwidth / low maintenance, costly

Local Back Up (Off-site archive)



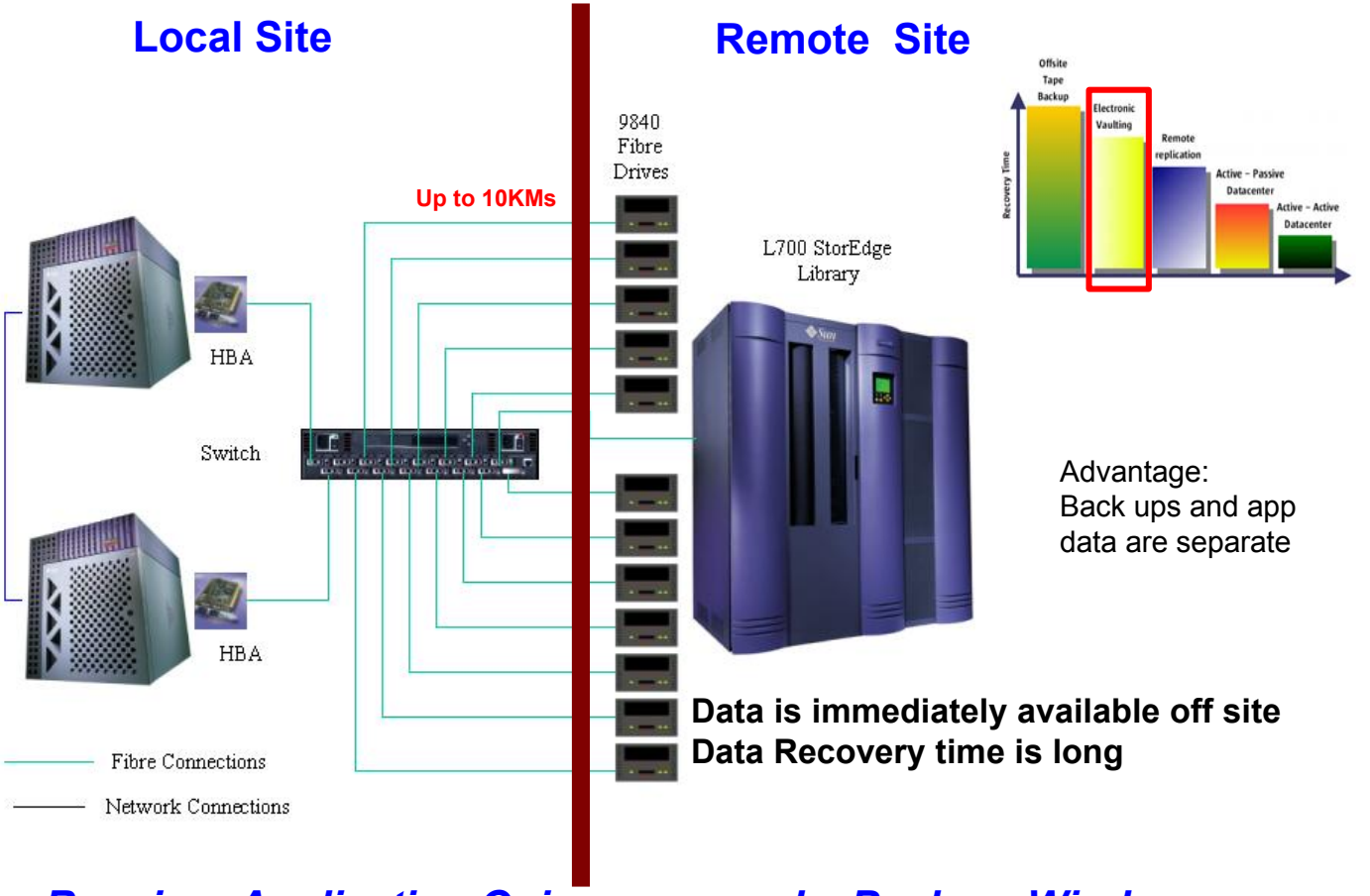


Manually move tapes offsite

Time to retrieve tapes
Time to retrieve data
Increases business recovery time

Requires Application Quiescence and a Back up Window

Basic Electronic Vaulting

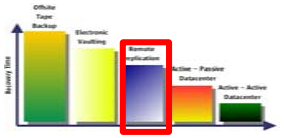


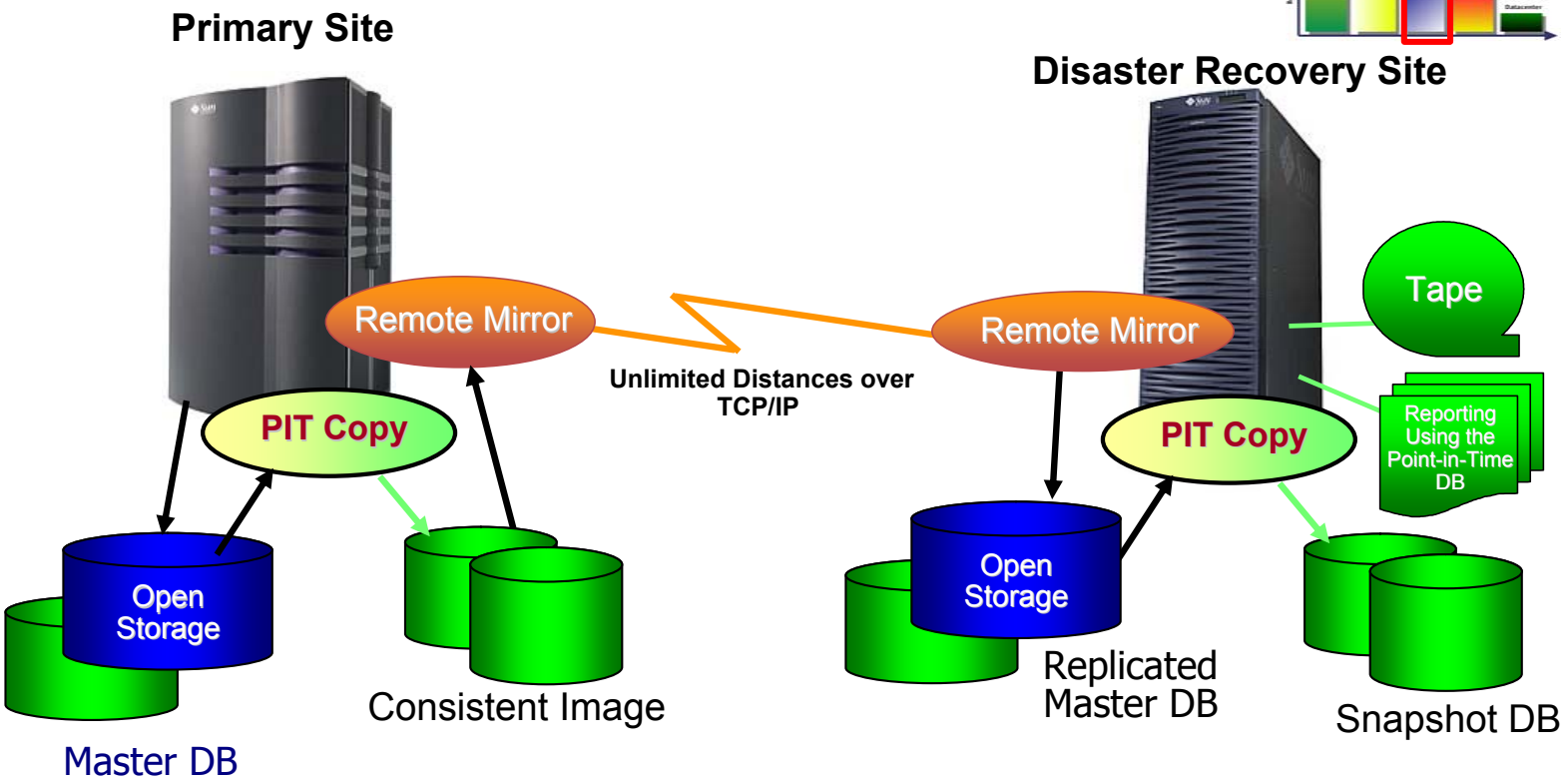
Advantage:
Back ups and app data are separate

Data is immediately available off site
Data Recovery time is long

Requires Application Quiescence and a Back up Window

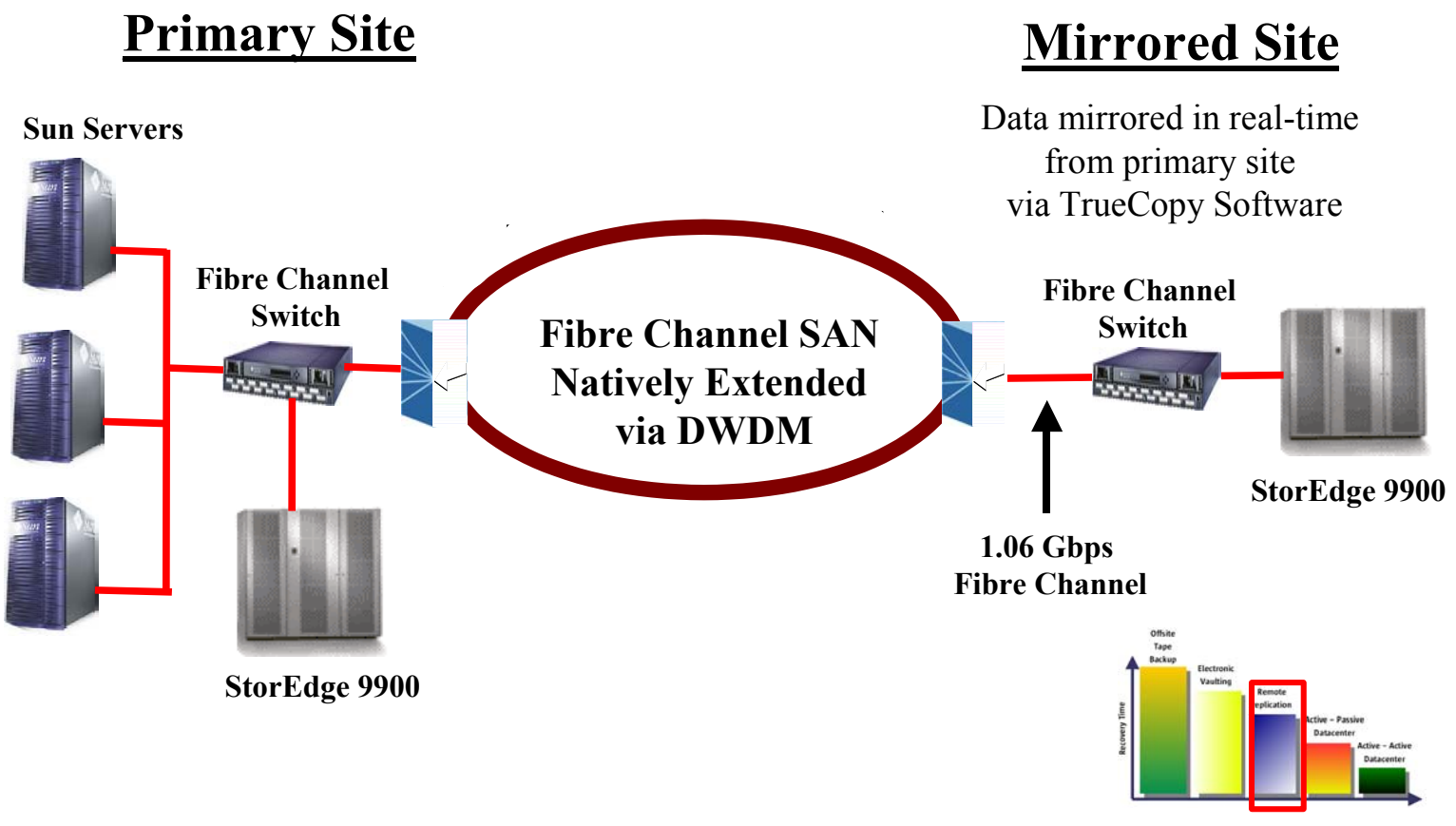
Host Based Data Replication



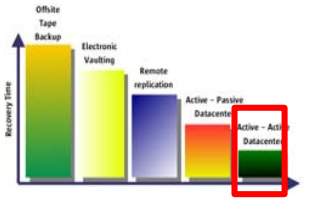


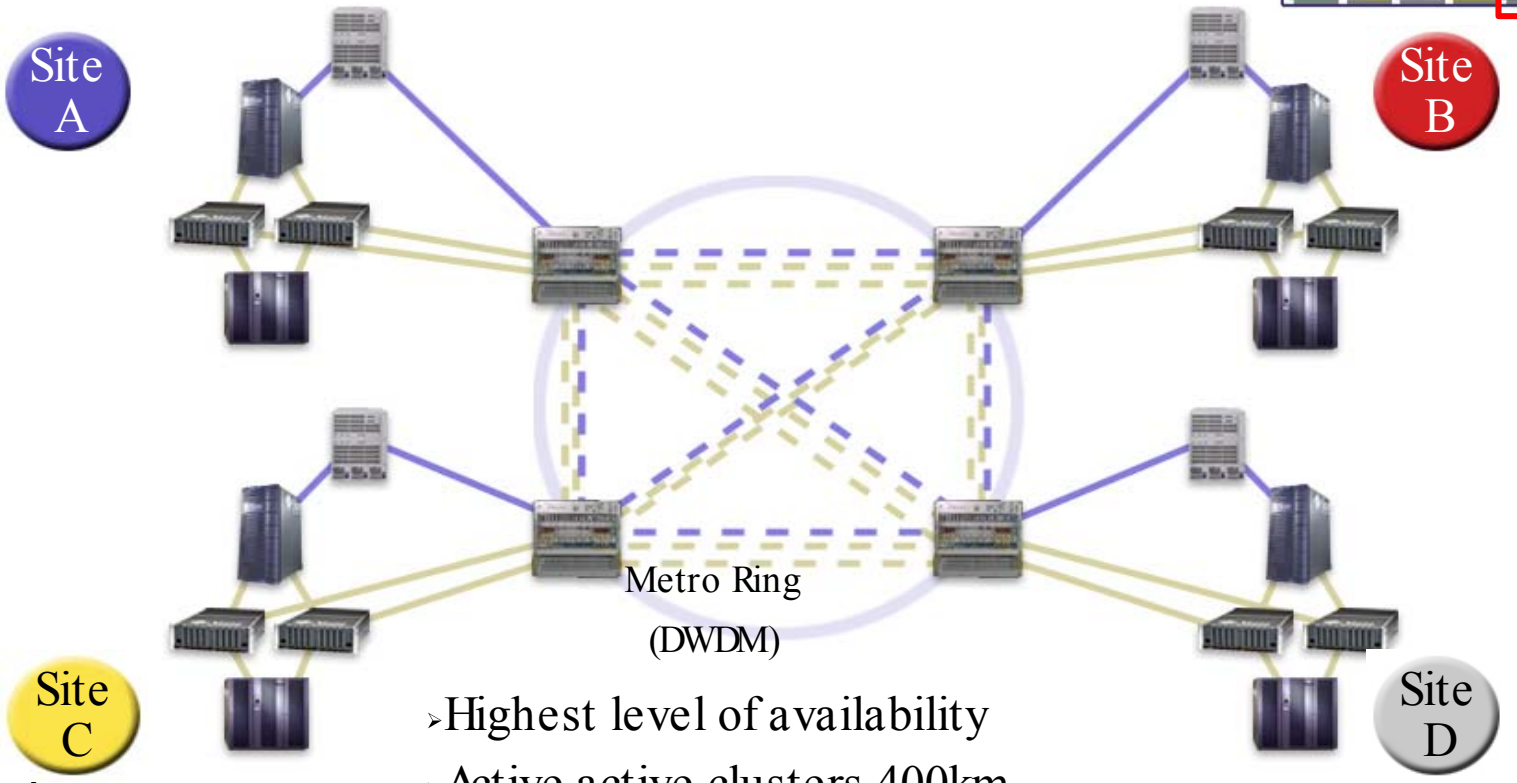
- Preserve a consistent data state at recovery site
- Use Disaster Recovery hardware for many applications

Storage Based Replication



Distance Clustering





- Highest level of availability
- Active-active clusters 400km

Summary

- Continuity planning is as important to government agencies as businesses
- You must plan…
- … and test your plan!
- There are multiple strategies for disaster recovery

Dick Kallmeyer

dick.kallmeyer@sun.com

1-510-574-6606

Sun microsystems

We make the net work.