Case Study: Business Continuity Planning for Site-Level Disaster

Kimberley Pyles

Lead, Engineering System Support
Northrop Grumman Corp.

HP WORLD 2003
Solutions and Technology Conference & Expo

Northrop Grumman Today

Positioned for Growth

- Strategic transformation from Aircraft Company to: Company to:
  - Electronic Systems – Ship Systems
    ms
    grated Systems – Space Technology
    gy

  ess record of integrating new businesses –
  ting-edge technologies - products in demand for

  ogies - products in demand for 21st century
  hting systems used in all environments from

  nments from beneath the sea to outer space.

  the sea to outer space.

Electronic Systems

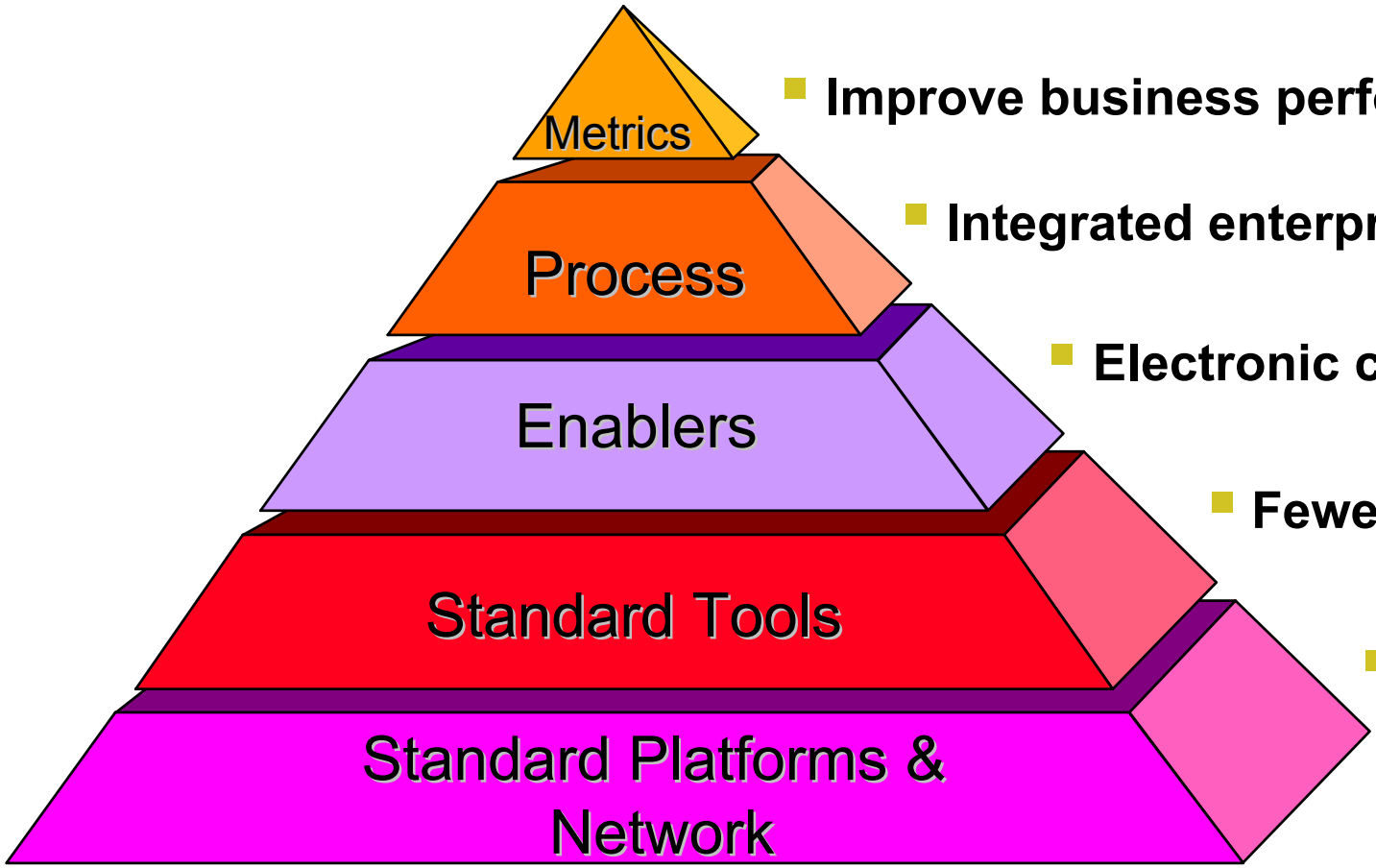
HP WORLD 2003
Solutions and Technology Conference & Expo

From Under Seas to Outer Space

- $ 6.1B - 2003E Sales
- 24,000 Employees
- 51 Major Operating Locations
- 19 International Offices
- Over 200 Key Programs
- More than 12,000 Active Contracts

NORTHROP GRUMMAN
Electronic Systems

Product Design Infrastructure …



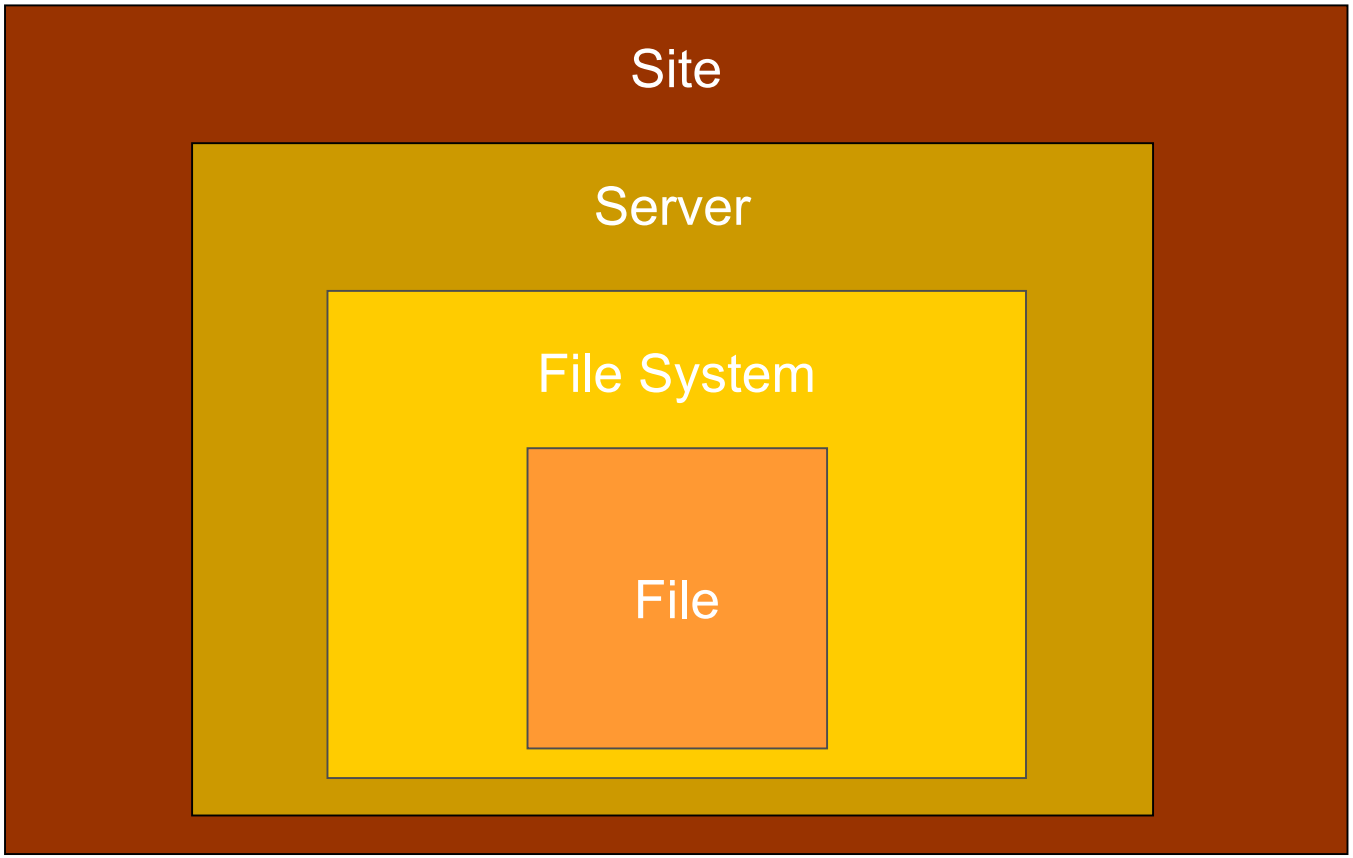
- Improve business performance
- Integrated enterprise process
- Electronic collaboration
- Fewer is better
- Single network

… Creates Building Blocks for Efficiencies and Improvement

Where we began…

- Corporate directive in 1999
- Started with Business Impact Analysis
- Tackled first: large, corporate-wide systems
- Tackling now: department/sector systems
- Complex plan based on assumptions and inter-related decisions
- Like an insurance policy

Scope of Disaster



Assumptions:

Site-Level Disaster

- Original site and systems are unusable
- Current administrators may not be available
- Corporate recovery team to handle infrastructure, networking, etc.
- End users may be at multiple sites

- Temporary recovery site while primary is restored
- Temporary servers at recovery site while purchasing permanent systems

Identify Processes

- Consider all processes in the life-cycle development of your product

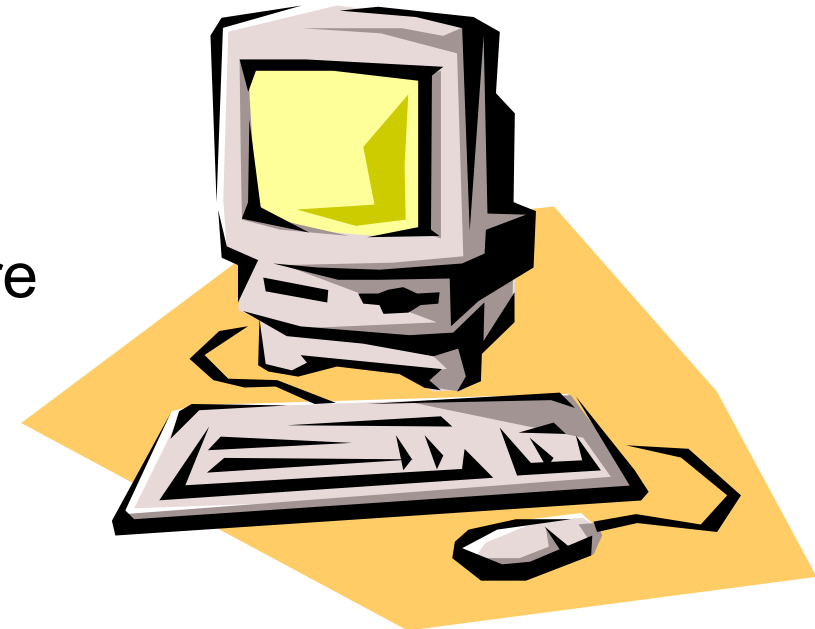
- Identify processes necessary to continue your business
- Rank processes by criticality

Identify Critical Data

- Identify data for critical processes
- Data form: electronic, paper, etc
- Loss affordability: lose a day, week, etc
- Data availability: need within a day, week, etc

Identify Critical Systems

- What systems support critical data
- Servers: file, license, application, compute, etc
- Clients:
  - PCs or UNIX workstations
  - Special software or hardware configurations



Site Recovery Strategies

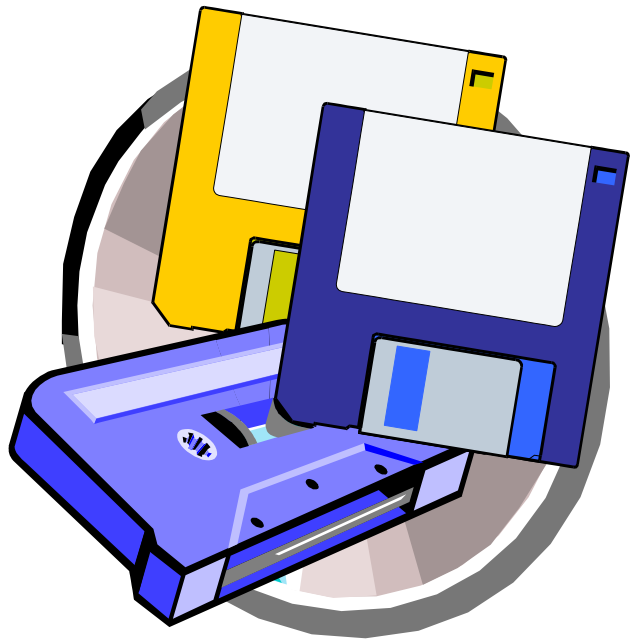
- **Hot**
  - Quickest fail over
  - Usually vendor recovery facility
- **Warm:**
  - Some infrastructure / systems available immediately
  - Data synchronization to slave server
- **Cold**
  - Infrastructure in place but not turned on
  - Company's remote site
  - Vendor mobile unit

Hardware Recovery Strategies

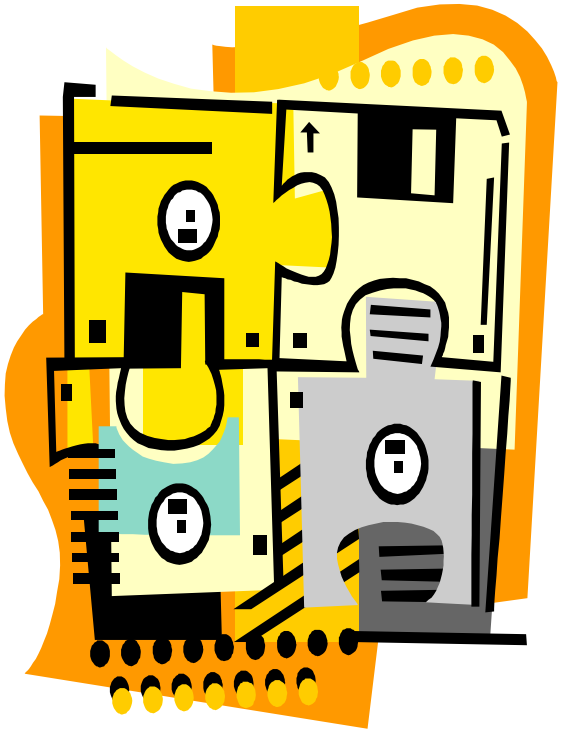
- Fail over to hot or warm site
- Quick-ship new servers and clients
- Stockpile servers and clients for older systems
- Consolidate servers

OS Recovery Strategies

- Restore image
  - Make recovery tape
  - Include application
- Recreate from scratch
  - Install from vendor media
  - Reconfigure system files



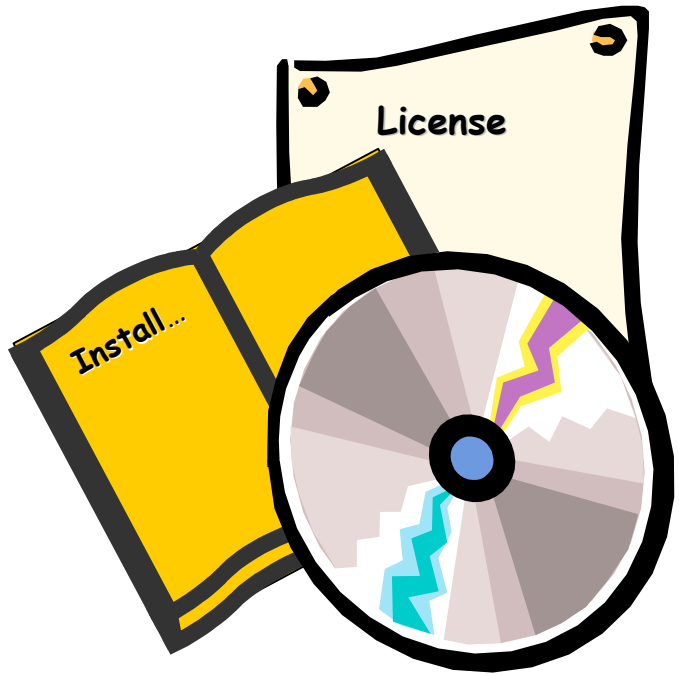
Data Recovery Strategies



- Synchronous updates
- Restore from backups
  - Full backups: point-in-time
  - Incremental/differential backups: nightly
  - Combination backups
  - OS vs third-party backup tool

Application Recovery Strategies

- Include application in OS image
- Load from scratch and configure
- Negotiate temporary license with application vendor

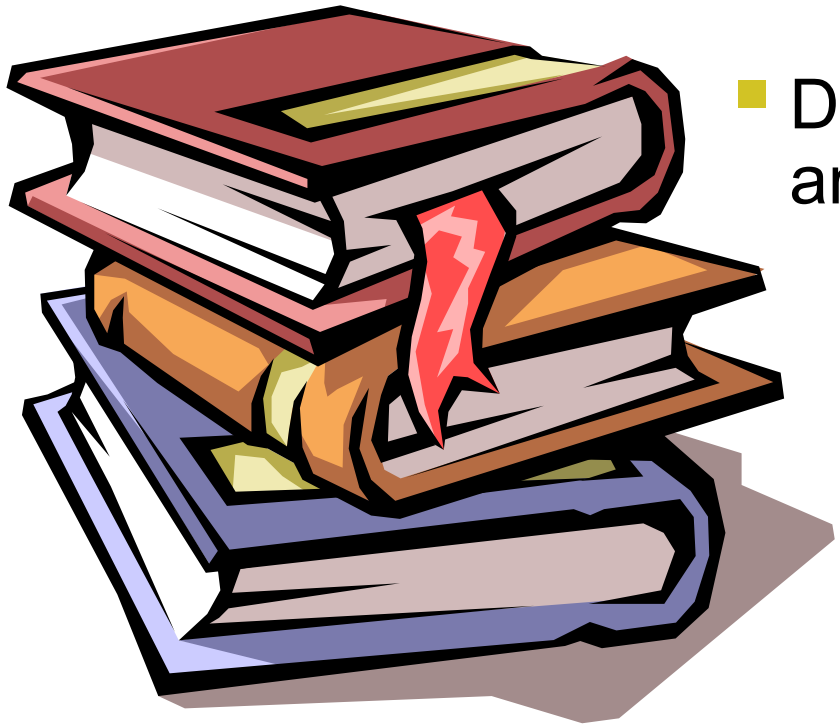


Cost of Recovery

- Infrastructure for recovery site
- Replacement systems for recovery site
- Replacement systems for permanent site
- Offsite data storage
- Labor to execute recovery plan
- Consulting fees

Documentation

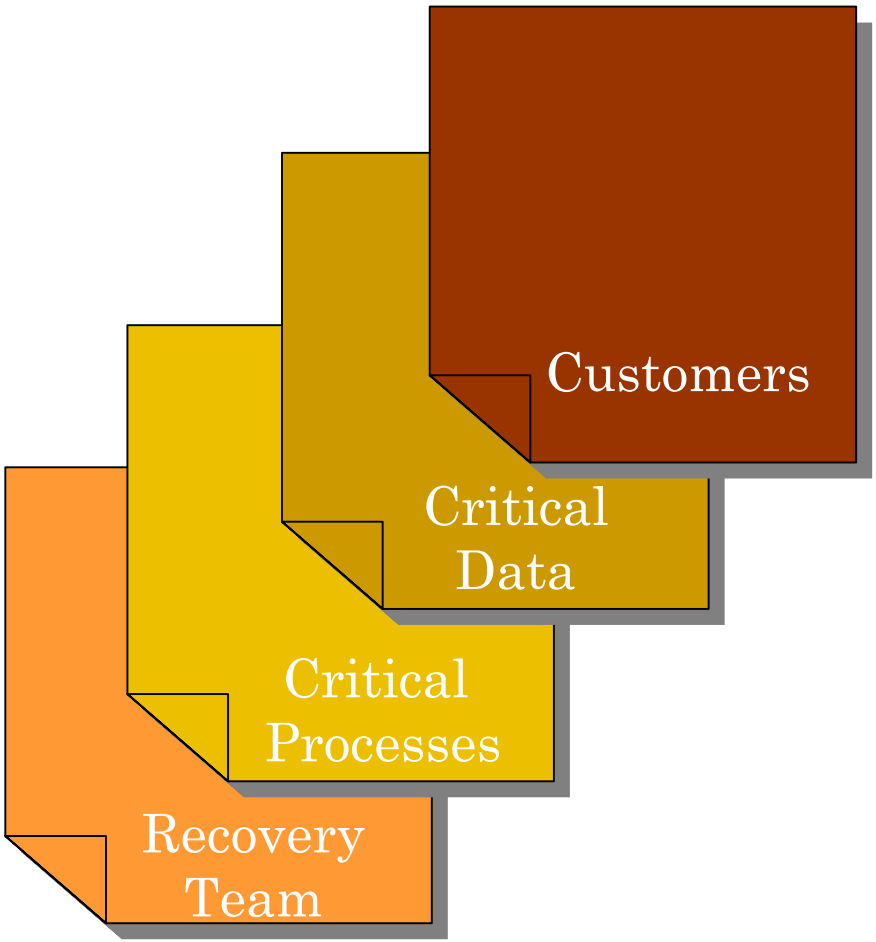
- List disaster assumptions.
  - Summarize disaster recovery strategy.

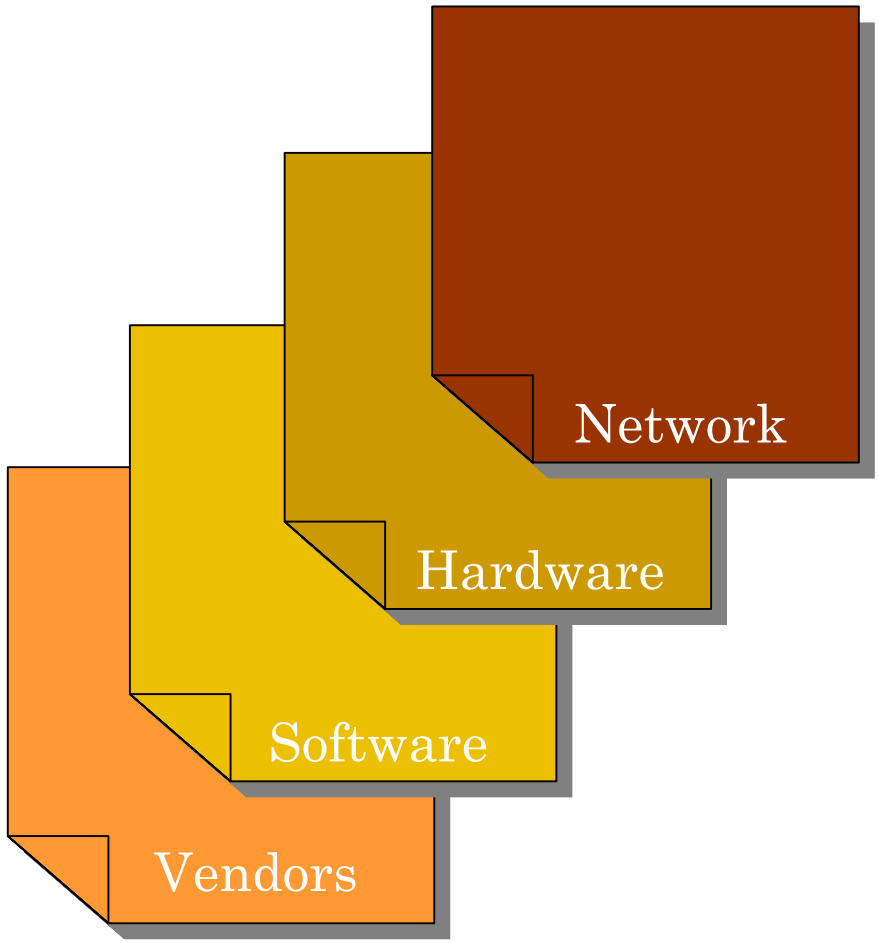


- Detail recovery steps so anyone can execute plan.
  - Include contact and support information.
  - Store recovery plan away from primary site.

Contact and Support Information

- Identify information to help execute recovery plan:





Testing

"No business continuity plan is valid until it has been tested." Kelly Williams & Meg Keehan, BCP Testing Techniques and Alternatives, March 2002

- Walk-through test
  - Partial at vendor site
  - Partial using alternate server
  - Full to validate documentation
- Table-top test
- Test all systems and applications
- Validate recovery documentation

Re-Evaluate Recovery Plan

- Test and validate plan periodically
- Test after adding or replacing systems
- Update recovery documentation
- Store updated recovery documentation offsite

Our Recovery Plan

- Cold site
- Quick-ship systems
- Load OS and apps from images
- Data and recovery plan stored offsite
- Restore data from full and incremental backups
- Detailed recovery plan
- Perform full walk-through test

If the disaster occurs…

- Rely on your recovery plan
- Know resources and use them
- Be flexible – but don’t cut corners
- Assess damage at original site
- Document changes to your plan

Questions

Interex, Encompass and HP bring you a powerful new HP World.