Disaster Recovery Planning for Manufacturing & Distribution Companies: Is Your Plan in Place?

David Dyk
Kevin Villanueva

MOSS ADAMS LLP
Certified Public Accountants | Business Consultants

PRESENTERS

David Dyk
IT Consulting
Moss Adams LLP

Kevin Villanueva
IT Consulting
Moss Adams LLP
The material appearing in this presentation is for informational purposes only and is not legal or accounting advice. Communication of this information is not intended to create, and receipt does not constitute, a legal relationship, including, but not limited to, an accountant-client relationship. Although these materials may have been prepared by professionals, they should not be used as a substitute for professional services. If legal, accounting, or other professional advice is required, the services of a professional should be sought.
AGENDA

• What is a Disaster?
• Disaster Recovery vs. Business Continuity
• Drivers for Having a Disaster Recovery Plan
• How Do You Get Started?
• Disaster Recovery Plan Structure
• Key Considerations
• Testing the DR Plan
• Resources
• Questions?
WHAT IS A DISASTER?

Sudden, calamitous event that brings great damage, loss or destruction. (Source: Merriam-Webster dictionary)

<table>
<thead>
<tr>
<th>Natural</th>
<th>Man-Made</th>
<th>Technological</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Earthquakes</td>
<td>• Power outages</td>
<td>• Database corruption</td>
</tr>
<tr>
<td>• Floods</td>
<td>• Sprinkler system bursts</td>
<td>• Viruses</td>
</tr>
<tr>
<td>• Storms</td>
<td>• Crime</td>
<td>• Internet worms</td>
</tr>
</tbody>
</table>
DISASTER RECOVERY VS. BUSINESS CONTINUITY

• **Disaster Recovery** – The process, policies and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organization after a natural or human-induced disaster.

• **Business Continuity** – The activity performed by an organization to ensure that critical business functions will be available to customers, suppliers, regulators, and other entities that must have access to those functions.
DRIVERS FOR HAVING A DISASTER RECOVERY PLAN

• High availability of data is required by your industry

• Regulatory requirements
  o Federal Emergency Management
  o Government Contractor

• Contractual obligation with a business partner
• Makes good business sense!
HOW DO YOU GET STARTED?

• Identify critical data
• Conduct a Business Impact Analysis (BIA)
• Create a data backup process
• Determine resources needed during a recovery effort
IDENTIFY CRITICAL DATA

Work with process “owners” in understanding their world and the critical data that is processed, transmitted, and stored.

✓ What type of data is required?
✓ From where do they acquire data?
✓ How is it acquired?
✓ Who is responsible for that data?
✓ When is the data acquired?
✓ Where is the data stored? (e.g., systems involved, storage area networks, other media)
BUSINESS IMPACT ANALYSIS (BIA)

• Purpose – To help organizations identify the business units, operations and processes essential to the survival of the business.

• Considerations:
  ✓ Life or death situation
  ✓ Potential for significant loss of revenue
  ✓ Obligations to external parties may be jeopardized

• RTO – Recovery time objective
• RPO– Recovery point objective
• Critical for determining the order and priority of system recovery
DATA BACKUP PROCESS

• Do you know if your data is getting backed up?
• How often is it getting backed up?
• Do you know where the data is being backed up? (network storage, tape media, offsite/onsite)
• How is the backup data stored and is it adequately secured?
• Work with IT staff to identify the critical system files that are required to recreate the data (includes database, operating system, application configuration data, etc.)
• Is the data restoration process being tested regularly?
DETERMINE RESOURCES NEEDED DURING A RECOVERY EFFORT

• Alternate recovery site (co-location facilities, hotel meeting rooms, executive suites, etc.)
• Server equipment (virtualized or physical, type/model, hardware configuration, storage equipment)
• How quickly can equipment be purchased and acquired?
• Software including operating system type, database environment, application, and configuration settings.
• Backup management software
• Backup media equipment (backup equipment – LTOs, SDLT, DDS)
• Connectivity (Internet, VPNs/links to partners, extranets)
• Critical IT staff (System Administrators, Database Administrators)
DISASTER RECOVERY PLAN STRUCTURE

• Assumptions (communications infrastructure in place, primary location still available, primary IT staff available)
• Roles and Responsibilities
• Declaration of a Disaster
• Equipment Salvage (procurement)
• System Recovery Process (alternate site)
• Resumption at Primary Site
• Declare End of Disaster (debrief)
ASSUMPTIONS

• Communications and infrastructure for the region is still functioning
• Key staff are available during the recovery effort
• Recovery procedures are sufficiently detailed so that external assistance can follow if needed
• Recovery of a subset of the system is adequate for business purposes
• There will be performance degradation and functionality may be limited
# ROLES AND RESPONSIBILITIES

The Disaster Recovery Team includes...

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disaster Recovery Coordinator</td>
<td>• C-level individual or Manager who directs the teams and serves as the leader of the recovery efforts</td>
</tr>
<tr>
<td>Media/Communications Representative</td>
<td>• C-level manager, legal counsel or similar spokesperson who ensures a consistent message is communicated to the media</td>
</tr>
<tr>
<td>Salvage Team</td>
<td>• IT and business unit staff who assess the equipment to determine if damage is minimal or extensive, and if new equipment needs to be procured</td>
</tr>
<tr>
<td>Recovery Team</td>
<td>• IT team responsible for system rebuilding and data restoration</td>
</tr>
<tr>
<td>Backup Support Staff</td>
<td>• The secondary individuals who can assume the role of the primary who may not be available</td>
</tr>
</tbody>
</table>
DECLARATION OF A DISASTER

• Criteria for invoking the disaster recovery plan
  ✓ Severe disruption to service
  ✓ Potential for major data loss
  ✓ Data security may have been compromised

• Initiating the call tree process
  ✓ Disaster Recovery Coordinator starts the notification and activates the other teams involved in the recovery effort
  ✓ Business unit managers responsible for notifying their teams

• Get the word out! (external website & intranet if both available, local media)
EQUIPMENT SALVAGE

• Primary site may be restricted from being accessed due to danger
• Survey damage to assets for insurance purposes
• Determine if anything can be saved or serviced by the vendor immediately
• Device/Server support agreements need to be leveraged
• Test potentially damaged systems before relying on them for recovery operations
• Initiate emergency procurement process for immediate hardware, software, and appliance needs
SYSTEM RECOVERY PROCESS (ALTERNATE SITE)

• IT team heavily involved with assistance from various operations teams depending on system being recovered
• Rebuild of makeshift network, including ensuring security from Internet-based threats
• Think about connections that need to rerouted or pointed to recovery site
• Acquire or rebuild server hardware and install base operating system and patches
• Install and configure application and database software
• Configure accordingly and test
• Initiate data restoration process
• Test processing functions with business unit representatives
• Get satisfactory response before deeming system operable and live in the recovery environment
RESUMPTION AT PRIMARY SITE

- Primary site has been declared safe by Fire Department, inspectors, other officials
- Connection to Internet and WAN have been re-established
- Replicate data back or move the recovery system for use as the primary system
- Re-establish connections or DNS pointers to primary site
- Test functionality with business process owners and get satisfactory response
DECLARING THE END OF THE DISASTER

• Communication to media, business partners, clients, other stakeholders
• Debrief with disaster recovery team members on what was good and where improvements need to be made
• Update the disaster recovery plan with new lessons learned
KEY CONSIDERATIONS

• Human safety is #1
• Data security
• Remote work access
• Equipment acquisition
• Media storage
• DNS
• Sufficient insurance
DISASTER RECOVERY PLAN – TESTING

1. Table top test
2. Structured walk-through
3. Parallel simulation
4. Live production simulation

- Test on an annual basis
- Keep your plan current
RESOURCES

• NIST Contingency Planning Guide for Federal Information Systems

• Disaster Recovery Journal – drj.com

• DRII the Institute for Continuity Management – drii.org

• Moss Adams IT Consulting Group – www.mossadams.com
QUESTIONS?

david.dyk@mossadams.com
503-512-0004

kevin.villanueva@mossadams.com
206-302-6542

Sign up for next month’s webcast
www.mossadams.com/events