100 years THAT COUNTS
1913–2013

Disaster Recovery Planning: Is Your Plan in Place?

Presented by:

Steve Shofner, CISA, CGEIT

MOSS-ADAMS LLP
Certified Public Accountants | Business Consultants

Acumen. Agility. Answers.

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 Disaster Recovery Plan
- Resources
- Questions?

DISASTERS

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

Natural

- Earthquake
- Flood
- Hurricane
- Drought
- Twister
- Tsunami
- Cold/Heat wave
- Thunderstorm
- Mudslide

Man-Made

- Riots
- War
- Terrorism
- Power outages
- Sprinkler system bursts
- Equipment sabotage
- Arson
- Epidemic
- Pollution
- Transportation accident
- Food poisoning

Technological

- Database corruption
- Hacking
- Viruses
- Internet worms

“DISASTERS” COME IN ALL SIZES

Small **Large**

OBJECTIVES OF DISASTER RECOVERY VS. BUSINESS CONTINUITY

- **Disaster Recovery** – Successfully recover IT systems in the shortest timeframe possible

- **Business Continuity** – Continue critical business functions in the absence of key resources (considering customers, suppliers, regulators, and others)

DRIVERS FOR HAVING A DISASTER RECOVERY PLAN

- High availability of data is required by your industry
- Regulatory requirements
  - Federal Emergency Management
  - Government Contractor
- Contractual obligation with a business partner
- Makes good business sense!

HOW DO YOU GET STARTED?

- Conduct a Risk Assessment
- Identify critical data
- Conduct a Business Impact Analysis (BIA)
- Create a data backup process
- Determine resources needed during a recovery effort

CONDUCT A RISK ASSESSMENT

Consider the risks to your organization and the probability of each happening:

Natural

- Earthquake
- Flood
- Hurricane
- Drought
- Twister
- Tsunami
- Cold/Heat Wave
- Thunderstorm
- Mudslide

Man-Made

- Riots
- War
- Terrorism
- Power outages
- Sprinkler system bursts
- Equipment sabotage
- Arson
- Epidemic
- Pollution
- Transportation Accident
- Food Poisoning

Technological

- Database corruption
- Hacking
- Viruses
- Internet worms

COMMON PLANNING PITFALL

- You do not need to develop individual contingencies for each type of risk/disaster.

- Focus on the absence of key resources, such as (but not limited to) data, regardless of the reason.

(for this presentation, we will focus on data)

IDENTIFY CRITICAL DATA (RESOURCES)

Evaluate processes with owners, identifying how/where critical data is input from, processed, stored, and exported to:

- ✓ What type (s) of data is required?
- ✓ What type(s) are key / critical?
- ✓ When, how, and where is data input from?
- ✓ Who owns that data?
- ✓ What processing happens with that data?
- ✓ Where is the data stored (e.g., systems involved, storage area networks, other media)?
- ✓ When, where, and how is data exported?

BUSINESS IMPACT ANALYSIS (BIA)

- Identifies 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
  - ✓ Quantify impacts where possible
- Determine:
  - ✓ RTO – Recovery time objective
  - ✓ RPO – Recovery point objective
  - ✓ Critical for determining the order and priority of system recovery

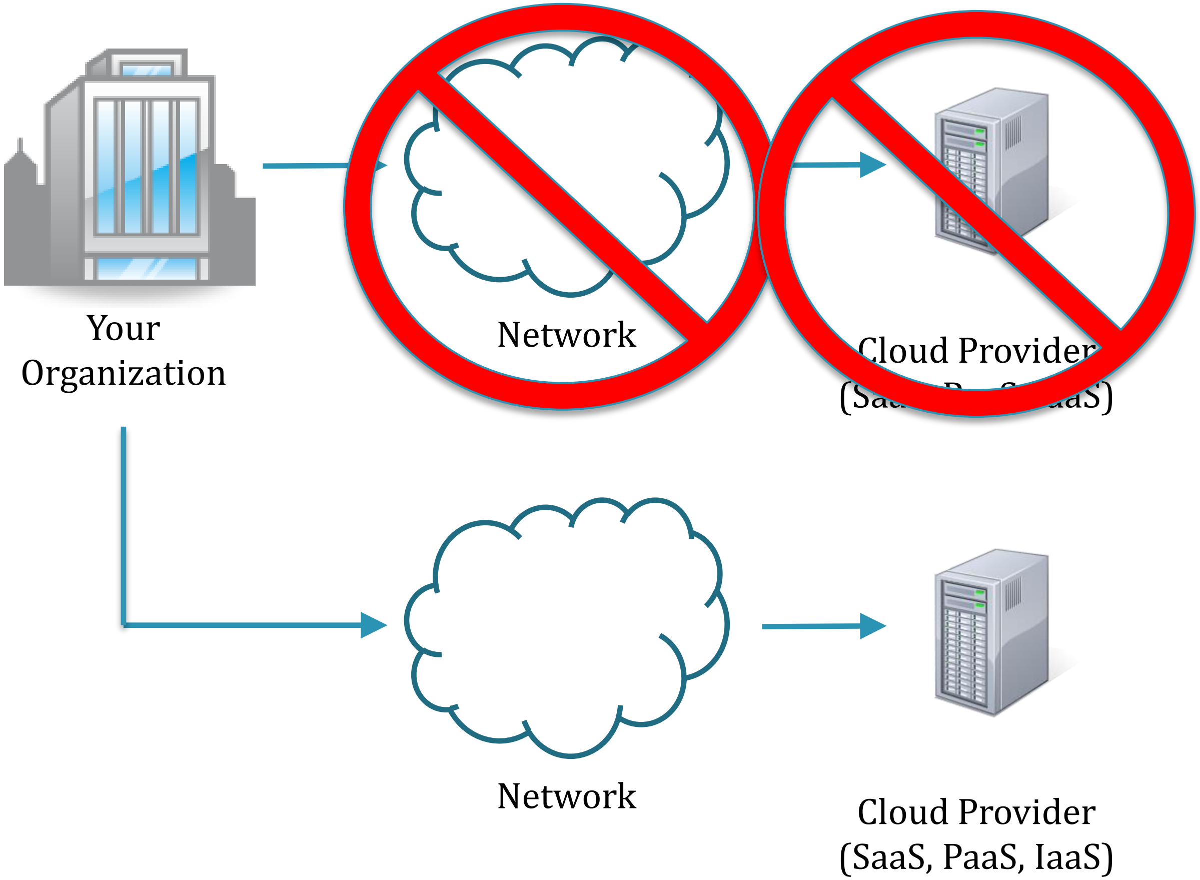
DATA BACKUPS

- Questions to ask:
  - ✓ Is your data backed up?
  - ✓ How often?
  - ✓ Where? (network storage, tape media, offsite/onsite)
  - ✓ How is it stored and is it adequately secured?
  - ✓ Is the restoration process tested? Regularly? How often?
- Work with IT staff to identify the critical resources required to recreate the data (includes hardware, database software, operating system, application configuration data, backed-up data, etc.)

IDENTIFY RESOURCES REQUIRED FOR RECOVERY EFFORT

- Alternate recovery site (co-location facilities, hotel meeting rooms, executive suites, etc.)
  - Hot / Warm / Cold?
- 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)
- Backup media
- Connectivity (Internet, VPNs/links to partners, extranets)
- Critical IT staff (System Administrators, Database Administrators)

CLOUD CONSIDERATIONS



Your Organization

Network

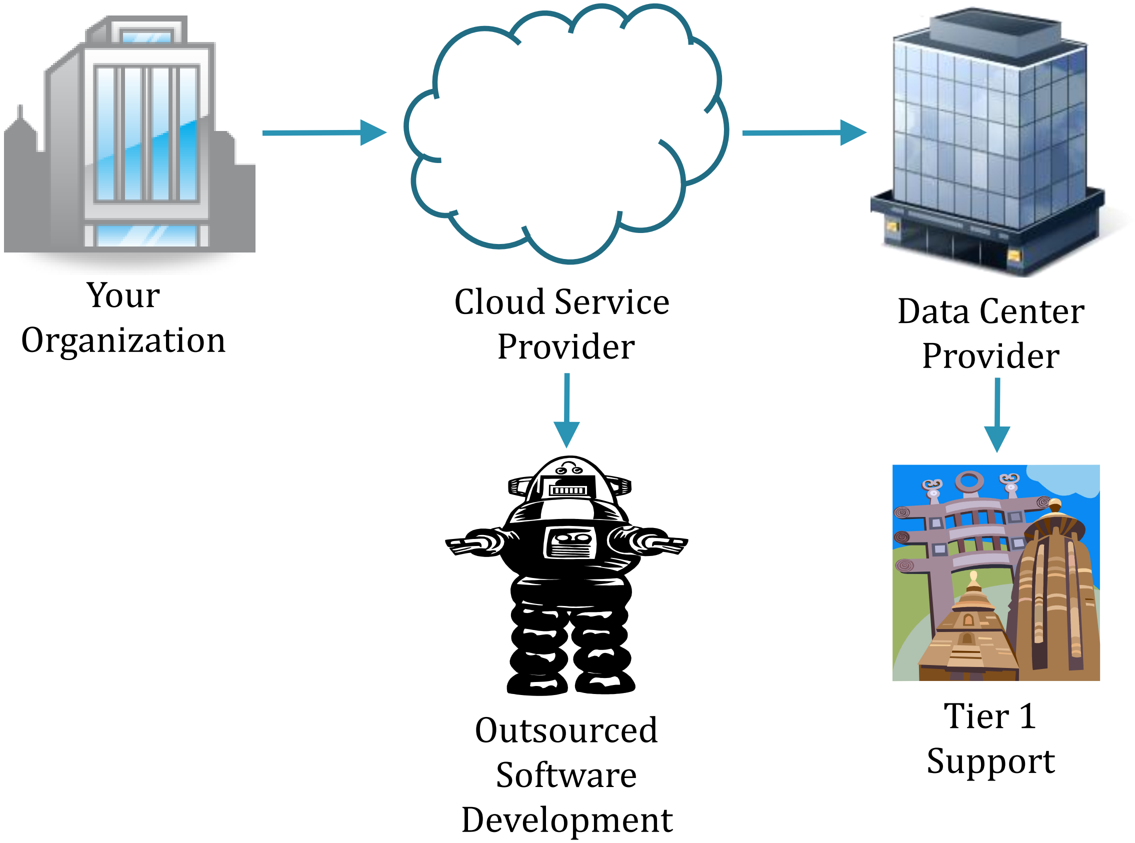
Cloud Provider (SaaS, PaaS, IaaS)

Your Organization

Network

Cloud Provider (SaaS, PaaS, IaaS)

CLOUD SERVICE CONSIDERATIONS



Your Organization

Cloud Service Provider

Data Center Provider

Outsourced Software Development

Tier 1 Support

CLOUD MANAGEMENT CONSIDERATIONS

- Understand the vendor’s environment
- Understand the vendor’s disaster recovery / business continuity plan
  - DR is often separate from service level agreements (e.g., 99.999% uptime) in many agreements, which often have disaster / force majeure (‘acts of God’) exceptions. Understand what guarantees they provide in DRP/BCP situations.
  - Obtain and *review* a Service Organization Controls (SOC) report
- Ensure there is an audit clause in your agreement

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)

CONSIDERATIONS

- Key staff (and/or vendors) may or may not be available during the recovery effort
  - Plan for Primary, Secondary, Tertiary, others
  - Ensure adequate decision-making and spending authority in advance
- Communications and infrastructure for the region may/may not be functioning
- Escalation plan and related timelines
- Recovery procedures should provide enough detailed so that alternate resources can follow if needed
- Recover all vs. subset of the required systems to meet critical (not all) business processes
- There will be performance degradation
- Functionality may be limited

ROLES AND RESPONSIBILITIES

The Disaster Recovery Team includes…

Disaster Recovery Coordinator	• C-level individual or manager who directs the teams and serves as the leader of the recovery efforts
Media/Communications Representative	• C-level manager, legal counsel or similar spokesperson who ensures a consistent message is communicated to the media
Salvage Team	• 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
Recovery Team	• IT team responsible for system rebuilding and data restoration
Backup Support Staff	• The secondary individuals who can assume the role of the primary who may not be available

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!

- Key Stakeholders:
  - Customers
  - Employees
  - Suppliers
  - Insurance providers
  - Civic agencies (e.g., Police, Fire, National Guard)
  - Local media

- Communication Channels:
  - Intranet
  - Externally-hosted website (consider mobile)
  - Phone
  - Automated phone service (call-out, dial-in, or both)
  - Print media
  - Mail
  - Bulletin board

DISASTER RECOVERY ACTIVITIES - EQUIPMENT SALVAGE

- Primary site may be available, but access is restricted 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

DISASTER RECOVERY ACTIVITIES - SYSTEM RECOVERY PROCESS (ALTERNATE SITE)

- IT team members are heavily involved with assistance from various operations teams depending on system being recovered
- Rebuild (makeshift) network, 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
- Consider controls (IT and non-IT)
- 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

DISASTER RECOVERY ACTIVITIES - RESUMPTION AT PRIMARY SITE

- Primary site has been declared safe by Fire Department, inspectors, other officials
- Connections 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

BUSINESS CONTINUITY

- Questions:
  - How will you continue delivering your process/service?
  - How will you manage employees (e.g., payroll)?
  - How will you manage vendors?
  - Others?
- Considerations:
  - Alternate manual/paper-based methods
  - Alternate controls (Financial, Operational, ITGCs, Security, etc.)

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

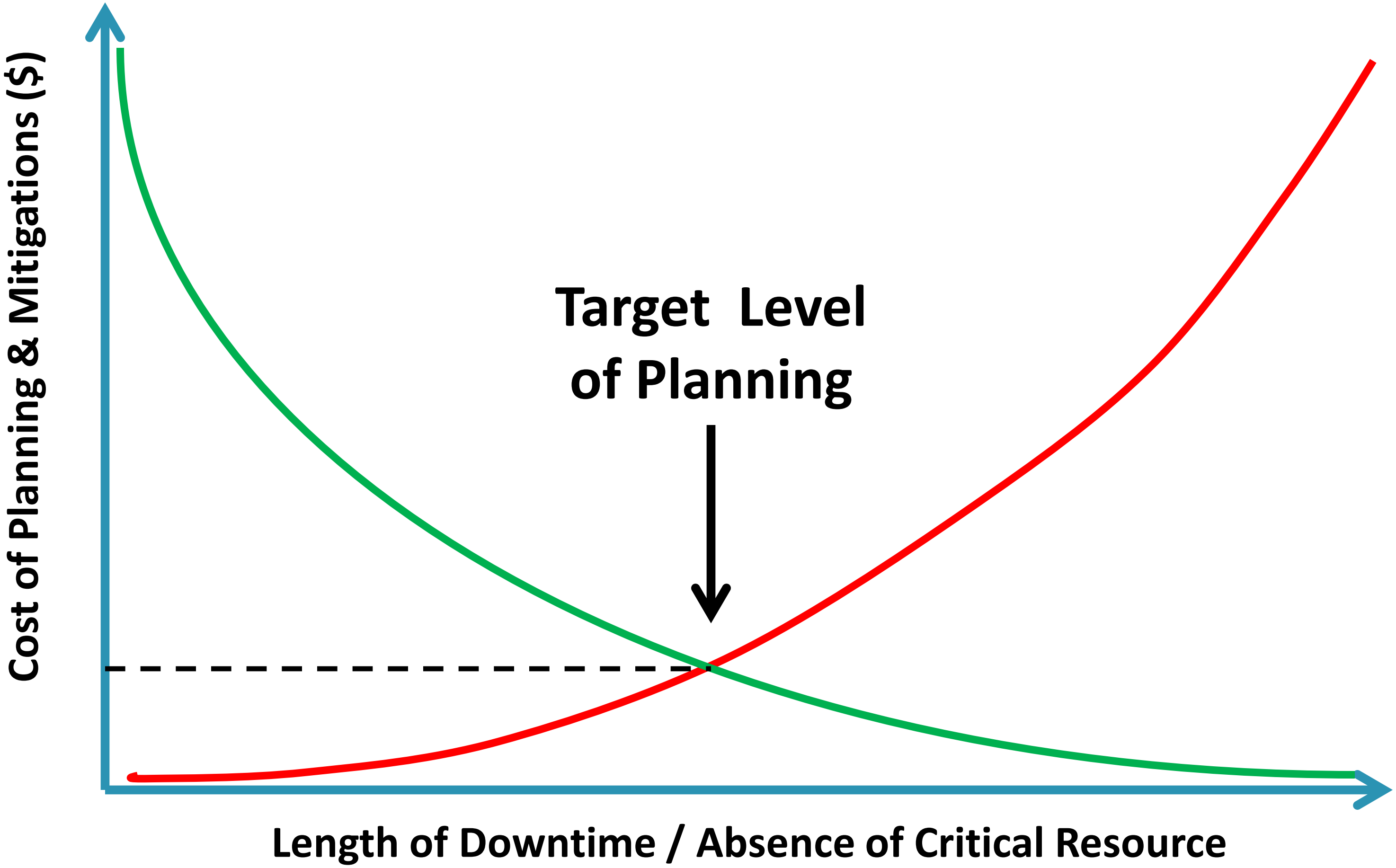
- Human safety is #1
- Data security
- Remote work access
- Equipment acquisition
- Media storage
- DNS
- Sufficient insurance

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
- Include all stakeholders (including vendors)

HOW MUCH PLANNING AND MITIGATION IS ENOUGH?



RESOURCES

- NIST Contingency Planning Guide for Federal Information Systems http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf
- Disaster Recovery Journal – drj.com
- Business Recovery Manager's Association – brma.com
- DRII the Institute for Continuity Management – drii.org
- Moss Adams IT Consulting Group – www.mossadams.com

PRESENTER

Steve Shofner, CISA, CGEIT

steve.shofner@mossadams.com

415-677-8263 (office)

510-681-6638 (cell)