Developing an Effective Disaster Recovery Plan

We will figure it out! or What is the point, anyway?

January 2017
MHA CONSULTING, INC.

KEY FACTS

17
Years in operation.

15
Average years industry experience.

CAPABLE
Comprehensive suite of services.

GLOBAL
Diverse, global client base.

SAAS
Compliance and risk tools.

• A 17-year proven track record of applying industry standards and best practices across a diverse pedigree of clients.

• A simple mission: Ensure the continuous operations of our client’s critical processes.

• Services include Business Continuity, Crisis Management, Disaster Recovery, IT Best Practices and Physical Security.

• SaaS tools include BCM Compliance and Residual Risk.

SENIOR LEADER

Richard Long
Practice Leader
Phoenix, Arizona
www.mha-it.com
<table>
<thead>
<tr>
<th>SERVICES</th>
<th>HEALTHCARE</th>
<th>EDUCATION</th>
<th>FINANCIAL INSTITUTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>EARLY WARNING services</td>
<td>AMGEN</td>
<td>ASU</td>
<td>American Express</td>
</tr>
<tr>
<td>LifeLock</td>
<td>CVS Health</td>
<td>Maricopa Community Colleges</td>
<td>PenFed Credit Union</td>
</tr>
<tr>
<td>ATS American Traffic Solutions</td>
<td>COVIDIEN</td>
<td>ASU</td>
<td>City National Bank</td>
</tr>
<tr>
<td>REDflex Traffic Systems</td>
<td>NUVasive</td>
<td>Johnson &amp; Wales University</td>
<td>Desert Schools</td>
</tr>
<tr>
<td>TransPerfect</td>
<td>McKesson</td>
<td>Apollo Group Inc.</td>
<td>Charles Schwab Bank</td>
</tr>
<tr>
<td>Hewlett Packard Enterprise</td>
<td>OhioHealth</td>
<td>The Catholic University of America</td>
<td>Charles Schwab</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CONSUMER PRODUCTS</th>
<th>INSURANCE</th>
<th>TRAVEL &amp; ENTERTAINMENT</th>
<th>GOVERNMENT/UTILITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>BJ's</td>
<td>Mutual of Omaha</td>
<td>MGM Resorts International</td>
<td>City of Tempe, Arizona</td>
</tr>
<tr>
<td>Ratner Companies</td>
<td>Health Alliance</td>
<td>Wells Resorts</td>
<td>PNM</td>
</tr>
<tr>
<td>Guitar Center</td>
<td>CopperPoint</td>
<td>Regal Entertainment Group</td>
<td>CAP</td>
</tr>
<tr>
<td>GameStop</td>
<td>Federated Insurance</td>
<td>Blue Cross Blue Shield of Arizona</td>
<td>IDAHO POWER</td>
</tr>
<tr>
<td>Insight</td>
<td>York</td>
<td>AAA</td>
<td>NASA</td>
</tr>
<tr>
<td>Nestle</td>
<td>TriWest</td>
<td>SkyWest</td>
<td>Clubcorp</td>
</tr>
<tr>
<td>PETSMART</td>
<td>Henkel</td>
<td>AAA</td>
<td></td>
</tr>
<tr>
<td>ProLogic</td>
<td>TriWest</td>
<td>AAA</td>
<td></td>
</tr>
</tbody>
</table>

© 2017 MHA CONSULTING. ALL RIGHTS RESERVED.
## COMPREHENSIVE SOLUTIONS PRACTICES

<table>
<thead>
<tr>
<th>Assess the Current Environment</th>
<th>Recovery Strategies/Solutions</th>
<th>Response &amp; Recovery Plans</th>
<th>Exercises</th>
<th>Maintain &amp; Improve</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current State Assessment</td>
<td>Business Recovery Strategies</td>
<td>Crisis Management</td>
<td>Training &amp; Awareness</td>
<td>Update Recovery Plans</td>
</tr>
<tr>
<td>Business Impact Analysis</td>
<td>Data Center Recovery Strategies</td>
<td>Business Recovery</td>
<td>Mock Disaster Exercises</td>
<td>Update Current State Assessment</td>
</tr>
<tr>
<td>Threat &amp; Risk Assessment</td>
<td></td>
<td>IT Disaster Recovery</td>
<td>Plan Functional Walkthroughs</td>
<td>Update Business Impact Analysis &amp; Threat Assessment</td>
</tr>
<tr>
<td>BCMMETRICS™ Compliance Confidence (C2)</td>
<td></td>
<td></td>
<td>Alternate Worksite Exercises</td>
<td></td>
</tr>
<tr>
<td>BCMMETRICS™ Residual Risk (R2)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© 2017 MHA CONSULTING. ALL RIGHTS RESERVED.
DEVELOP AN EFFECTIVE DISASTER RECOVERY PLAN

- Why plans and documentation are necessary.
- Strategies to develop the documentation.
- Integration with Business Continuity Plans.

PROVIDE USABLE & EFFICIENT INFORMATION AND INSTRUCTIONS

- For accurate and reliable recovery of technology:
  - Necessary content.
  - Organization of the content.
  - Exercise options and strategies.
  - Keeping the documentation relevant.
THE BIG PICTURE

Risk

Resilience

Maturity

Compliance

Readiness
DEFINITIONS

RECOVERY TIME

OBJECTIVE VS. ACTUAL
TIME TO RECOVER ENVIRONMENT

Recovery Time Objective
• Desired state – business requirements.

Recovery Time Actual
• Current capability provided by IT.

RECOVERY POINT

OBJECTIVE VS. ACTUAL
ACCEPTABLE DATA LOSS

Recovery Point Objective
• Desired state – business requirements.

Recovery Point Actual
• Current capability provided by IT.
WHAT IS A DISASTER RECOVERY PLAN?

- All the necessary information to effectively recover the technical environment to support business functions during an outage event.
- There are typically multiple plans associated with disaster recovery.
- Consider the disaster recovery plan as the overall strategy and high-level order of system, technology and application recovery.
- Often, each technology or environment will have an individual technical recovery plan.
- Both the high level and individual plans should be formal and reviewed documents.
- Regular (annual) updates are recommended. Upon significant changes to the environment, the plan should be updated as part of the production implementation.
WHY RECOVERY PLANS?

WHY SPEND TIME DEVELOPING PLANS?

• DR is dead – most of our apps are in the cloud.
• Our technology team knows what to do.
• We will figure it out.
• Recovery is automated/scripted. We really only “click a few buttons.”
WHY RECOVERY PLANS?

**DR IS DEAD**

- Most events are self-inflicted (recent airline outages).
- Unanticipated events – not natural disasters.
- Customers will NOT understand.
WHY RECOVERY PLANS?

THE TEAM WILL KNOW HOW TO EXECUTE

• People are good at what they do every day. You don’t recover every day.
• They will be tired or trying to perform multiple recoveries.
• You may be using secondary resources or contractors.
WE WILL FIGURE IT OUT

• True, but that will take time. Your strategy to meet RTO/RPO is mostly likely based on best case.
• There will be unexpected issues even in best case.
• Often the actual recovery time does not meet the RTO. Time is almost always a limiting factor.
• Often the recovery environment is not completely in sync with production.
DEVELOPMENT STRATEGIES

HOW TO
DEVELOP PLANS?

- Use current documentation.
- Leverage production changes (implementations or new functionality testing).
- Document during exercises.
- Phased approach – start high level, then develop detail.
DEVELOPMENT STRATEGIES

USE EXISTING TASKS WHEN DEVELOPING PLANS

- **Production Implementations/Changes**: Modify any documentation used for production implementations or testing related to changes in environments as a basis for recovery or validation tasks. Architecture or systems overviews may be available as well.

- **Technology Testing/Validation**: These will often have relevant tasks or environment information which should be included in the documentation. Environment-specific tasks based on the implemented architecture are often found during these tests.

- **DR Tests**: As time has been allocated to perform the testing, use this time to take screens shots, note specific tasks and exceptions. Even if plans have been developed, this is where functional information will be identified.

- **Current Documentation**: Review and either update or reference current documentation. This is especially useful for architecture, server and storage details, as well as personnel responsibilities and contact information.
WHAT CONTENT SHOULD BE INCLUDED?

- Institutional information.
- Technology or environment-specific information.
- Exceptions.
- Integration between systems.
- Special configuration or settings.
- Validation steps (more than just the tools shows “green”).
- Architecture information as a reference.
- Personnel needed.
Often documentation is based on testing and not what will occur in a real event.

Include all necessary servers, storage, technologies (e.g., load balancers, all remote access environments).

Third party dependencies.

Integration/communication between recovery sites.
INCLUDE SPECIFIC

INSTITUTIONAL & TECHNOLOGY INFORMATION

- Specific settings or needs based on your organization’s requirements – e.g., security settings which may be more restrictive, naming conventions that may be confusing, shared environments (DB/App).

- Technology states – e.g., storage use which may raise concerns, special server settings, non-standard use of technology.

- Supporting technologies that are critical to recovery (authentication, load balancing).

- Manual steps due to non-critical administrative tools.

- Exceptions to processes or processing:
  - Changes in backups, performance, availability.
VALIDATION STEPS

• List the condition of the technologies in detail:
  • Expected memory, CPU, storage.
  • Number of servers per VM host.
  • Services or processes which should be running.
  • Connectivity.

• Do NOT assume just because an environment is “up” everything is correct.

• 15 – 30 minutes of time spent verifying expected states will save hours of troubleshooting and frustration by non-IT personnel.
INTEGRATION

• What are the integration technologies?
  • File-based, API, DB connections.
  • FTP, VPN, direct.

• Timing of data movement.

• Data synchronization state.

• Steps to rerun or update data to ensure systems are in sync.

• Third party connections.

• Communication steps or milestones based on dependencies.
HOW SHOULD CONTENT BE ORGANIZED?

• Actionable content – at the beginning of the document.
• Checklist based – limit narrative.
• Reference and audit information – in appendices.
• Architecture information – in appendices.
## Table of Contents

### I. PLAN OVERVIEW
- A. System / Application Description
- B. Recovery Strategy

### II. ENVIRONMENTAL AND INFRASTRUCTURE RESTORATION
- A. Environmental Recovery Action Tasks
- B. Operating System Restore/Recovery Procedures or Scripts

### III. FUNCTIONAL RESTORATION
- A. Functional Recovery Action Tasks and Dependencies
- B. Data Base Restore/Recovery Procedures or Scripts
- C. Application Restore/Recovery Procedures or Scripts

### IV. DATA RECOVERY/SYNCHRONIZATION AND BUSINESS VALIDATION
- A. Data Recovery/Synchronization Action Tasks
- B. Data Recovery/Synchronization Procedures or Scripts
- C. Business Validation Tasks
- D. Business Validation Procedures and Scripts

### V. RESUME PROCESSING
- A. Action Tasks
- B. Post Turnover Tasks
- C. Deviations to Normal Operating Procedures

### VI. RETURN TO PRIMARY SITE
- A. Approach for Returning to Normal Business Locations

### VIII. APPENDICES – INFORMATION IN SECTIONS BELOW MAY IN LINKS TO OTHER DOCUMENTS
- A. Plan Information
- B. Recovery Team Member Roles and Skill List
- C. Offsite Storage Information
- D. Backup and/or Replicated Information
- E. Hardware Mapping Between Primary and Failover Site
- F. Hardware/Software Primary Site Configurations and Requirements
- G. Hardware/Software Failover Site Configurations & Requirements
- H. Department Work Requirements (Forms/Documentation/Workstations)
- I. Critical Functions and Inputs/Outputs/Dependencies
- J. Recovery Timeline and Plan Assumptions
INTEGRATION WITH BUSINESS CONTINUITY PLANS

CHECK YOUR

BUSINESS CONTINUITY PLANS

FOR RELEVANT INFORMATION

• Access methods to environment(s).
• Number of individuals who will access over time (each day or over the course of the event).
• Changes to business processes.
• Technology that needs to be recovered that may not be included in the IT DR listing:
  • Security keys.
  • Remote access requirements (Citrix, RDP or department specific).
  • Shadow IT-based technologies or apps.
• More frequent tests with individual or several environments.
• Secondary resource execution with primary resource “not available.”
• Tabletop plan review with secondary resources to review documentation.
• Plan review as part of change control.
• Include plan review as milestone in production change or implementation project plans.
SO, WHAT ARE THE NEXT STEPS?

WHAT DO WE DO NOW?
HOW DO WE START OR CONTINUE?

• Prioritize development based on environment criticality.
• Develop recovery tasks, then validation tasks.
• Environments that do not have documentation.

AREAS TO REVIEW
WHERE TO PRIORITIZE

• Base infrastructure (server, VM, network, authentication).
• Integrations.
• Technology gaps.
• Resource constrained areas.
• SaaS/IaaS environments.
• Validate recovery strategy.
THINGS TO THINK ABOUT

- **Consider** your organization and where you can leverage time and content for documentation rather than adding an additional task.
- **Prioritize** the content based on the important information.
- **Develop** a high-level run book based on technology dependencies, application dependencies, RTOs and potential resource constraints.
- **Checklist-based** with reference to current documentation. Limit duplicate copies of information/data.
- **Perfect** is the enemy of the good. Something is better than nothing.
- **Focus** on the outcome, become **target focused**, and concentrate on the ability to **successfully recover**.
FINAL THOUGHTS

That’s been one of my mantras - focus and simplicity. Simple can be harder than complex: You have to work hard to get your thinking clean to make it simple. But it’s worth it in the end because once you get there, you can move mountains.

(Steve Jobs)
SUMMARY

• Documentation is important due to unforeseen circumstances, potential staffing issues, recovery time requirements, etc.

• Use current documentation, technology validation tests, implementations, etc.

• Include proprietary information, environment-specific information.

• Actionable information at the front of the documentation, informational, audit data in appendices.

• Reference Business Continuity information in the plans in summary.
UPCOMING WEBINARS

• CALCULATING BCM ROI, Michael Herrera
  – WEDNESDAY MARCH 8, 2017 AT 11:00 A.M. PST