Disaster Recovery Planning – Leveraging the Cloud
AGA Central Ohio Chapter, October 23 – 24 Columbus, OH

Agenda
• What
• How
• Where

Disaster
What is the definition of an “IT Disaster”?
• An unplanned incident that causes an interruption to normal business due to the loss of access to computer resources at some or all facilities
• Relocation of systems to a standby facility must be considered.

What constitutes a Disaster?
• Common causes... But most recently Malware/ Ransomware and Distributed Denial of Service

✔ Power outages 28% Hurricanes 6%
✔ Storm Damage 12% Fires 6%
✔ Floods 10% Software Error 5%
✔ Hardware Error 8% Power surge/spike 5%
Physical Attack 7% Earthquake 5%
Business Continuity (BC) vs. Disaster Recovery (DR)

- Business Continuity (BC):
  - All business functions (IT and non-IT) of the organization as a whole.
  - Includes risk assessment, and plans for functional units and business processes.
  - Potentially wider variety of scenarios.
- Disaster Recovery (DR):
  - IT activities to enable recovery to an acceptable condition.
  - BC encompasses DR.

Quick poll

1. Anyone have a business continuity plan?
2. Anyone have a disaster recovery plan?
3. Is everyone backing up their servers and computers? Everything on them?
4. Regular testing for backups (system restores)?

What is a DR Plan and Where do I Start?

- What is DR Plan?
  - Defines a set of coordinated processes and procedures for restoring systems, data, and infrastructure required to support key business operations.
- Where do I Start? – the very simple version!
  - Understanding your data by talking about the systems you use
  - Prioritize your data by understanding your mission
  - Not all data is equal or should be treated equal, unless money is no object!
  - Build a plan that keeps you safe
Structured framework

1) Management Commitment
2) Planning/Steering Committee
3) Risk Evaluation
4) Business Impact Analysis
5) Determine Recovery Strategy
6) Data Collection
7) Develop Emergency Operations Center

DR Planning Process

Threat & Risk Analysis
- Identify probable and impactful threats
- Define a calibrated risk

Business Impact Analysis
- Identify keys applications & systems
- Determine the recovery priority & timing

Risk Management
- Identify the recovery strategies
- Define the recovery approach specific scenarios

Business Impact Analysis (BIA)

- Purpose
  - Document critical business processes and determine recovery priorities
  - Inventory applications and business processes used by departments and business units
  - Dependencies and criticalities for applications and processes

- Outcome
  - Demonstrate the costs of interruption to critical services
  - Highlight the relationships between critical business processes and supporting applications and infrastructure
  - Document Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)
Sample RTO/RPO Matrix

What is an optimal DR Plan?

Common Mistakes on DR

1) Lack of understanding of business
2) Viewed as a technology only project
3) Documents are too complex
4) Not one and done!
5) Untested plan
6) “Never happens to me”

Overcome them by...

1) Readiness assessment
2) Integrated with business
3) Defined execution
4) Flow is critical
5) Training & testing
6) Change management process
Location, Location, Location

**Onsite (Local)**
- **Benefits:**
  - Inexpensive
  - Complete backup
- **Drawbacks:**
  - No protection against site failure
  - Difficult to monitor

**Offsite (Manual)**
- **Benefits:**
  - Inexpensive
  - Complete backup
  - Protects against site failure
- **Drawbacks:**
  - Unreliable, many manual processes
  - High legal risk
  - No monitoring
  - Significant downtime

**Hot Site**
- **Benefits:**
  - Complete backup
  - Protects against site failure
  - Reliable
  - Low downtime
- **Drawbacks:**
  - Complex
  - Significant planning
  - Requires monitoring
  - High investments
  - Requires training

**Cloud**
- **Benefits:**
  - Protects against site failure
  - Low intervention
  - Flexibility
  - Low downtime
  - Monitored
- **Drawbacks:**
  - Selective data
  - Significant diligence required
  - Can be expensive

---

**DR Architectures**

---

**Increasing adoption of cloud for BC/DR**

**Challenges of traditional DR**
- **Expensive**
  - Often requires duplicate IT infrastructure, silos of management
  - Fixed system capacity and costs
- **Complex**
  - Complicated system configuration
  - Many manual processes and procedures
  - Requires specialized knowledge and staff
- **Unreliable**
  - Testing may not always be completed
  - Time consuming to monitoring

**Advantages of cloud DR**
- **Cost Effective**
  - Can provide a pay-as-you-grow model
  - Shifts costs from non-recurring to recurring costs
- **Efficient**
  - Provides simplified management and support model
  - Ability to leverage provider expertise and specialized knowledge
- **Reliable**
  - Allows for frequent and non-disruptive testing
  - Provider SLAs for RPOs & RTOs
Increasing adoption of cloud for BC/DR

As organizations continue to embrace their cloud strategy and become more mature, their benefits increase accordingly. Dabbling or “exploring” cloud solutions inhibits your ability to truly realize many of the benefits.

Cloud Based Architecture

Challenges - Cloud Management
- Planning
- Procurement & Contracts
- The human element
- Security
- Cloud lifecycle
The Cloud Journey

- May require significant time and effort relative to the size and complexity of the environment and business objectives.
- A clear understanding of your needs and the problem to be solved by the cloud.
- Set reasonable timelines and organizational expectations for your cloud initiatives.

Plan and Check

- Requires careful upfront planning and should use a phased approach.
- Mapping business objectives to services (e.g., disaster recovery) is key to developing the requisite architecture – the 3 "R's" (redesign, replace or remain).
- Often a blended provider approach is required for a complete solution.
- Sometimes changes in required services can have contractual implications, monthly costs constraints or costly termination fees.

Procurement & Contract Terms

- Different procurement methodology
- Contracts meets near term and long term needs.
- Striking balance between MRC vs NRC
- Evaluate Total Cost of Ownership
- Breaches and definition of responsibilities
- Setting clear expectations and formalize them into contractual documents
- Define provider SLA’s that align with your own.
- Financially backed SLA’s.
- Understand what is not included
- Data locality & data duplication requirements.
What if…

- Difference in Contracted Solution vs. Delivery
- Unsustained SLA?
- Establish disentanglement criteria upfront and extraction of hosted data.
- Clear understanding of the termination clauses and costs.
- Understand ownership of equipment, software and licensing.
- Make sure you own your data and that it is accessible.

The Human Element

- Different skill set required to manage a cloud architecture.
- Managing cloud architectures requires a different skill set than an on premise architecture.
- Role of IT evolves from operation to business analyst, vendor broker and focus on delivering value to the business.
- Equipment huggers reluctant to relinquish duties and responsibilities to an external provider.
- Service provider becomes an extension of your IT organization.

Security Considerations

- Data guardianship and management can become complex.
- Validation of the provider’s security policies.
- Visibility and control of core infrastructure security.
- Compliance considerations - PCI-DSS, HIPAA, FEDRAMP, EU-US Privacy Shield, etc.
- Provider technical fit & non-technical fit (culture).
- Ask questions!
The Cloud Lifecycle

- Cloud requires continual care and feeding.
- The operations & provider management aspects often get overlooked with the focus simply being on “getting there” and may change as needs change.
- Changing needs and contractual terms make this process cyclical.

Successful Partnership...

1) What problem am I looking to solve?
2) How will I effectively use cloud services to accomplish my goals?
3) Do I have the right staff and technical expertise & how will our needs change?
4) Is a blended or multivendor approach necessary?
5) Are my potential provider(s) a good fit both technically and culturally?
6) Is my role and that of my provider clearly defined?
7) Have I set clear expectations for a trusted provider?
8) Do I have the complete financial picture?
9) Is my contract and MSA mutually beneficial?
10) What’s my exit strategy?

Questions
Know you can recover rather than thinking you can!