Disaster Recovery and Business Continuity

Ricky Smith • Innovative Business Technologies, Inc.

Agenda

• Introduction
• Causes of Data Loss
• Impact of Data Loss and Downtime
• Risk Analysis
• Data Retention
• Data Protection Methods
• Components of a Business Continuity Plan
• Online Resources and Tools
• Q&A

Introduction

About me

• President, Innovative Business Technologies, Inc.
• Director of Technical Services, McKesson Information Solutions Homecare and Hospice
• Systems Engineer, B.T. Alex. Brown
• Systems Engineer, Millennium Inorganic Chemicals
Causes of Data Loss

- Natural disasters
- Local structure incident
  - Fire
  - Water exposure
- Human error
  - Accidental overwrite or deletion
- Malicious Software
  - Virus - Corruption or deletion
  - Ransomware
- Failed upgrades
- System outage
- Fire
- Water exposure
- Human error
  - Accidental overwrite or deletion

What about inaccessible data?

- Field Staff
- Web Based Portals
  - Patient
  - Physician
  - Employees
- Emergency Preparedness
- Causes
  - Network based attacks (DDOS)
  - ISP outages
  - Power grid issues

Impact of Data Loss and Downtime

Average Downtime Cost Per Hour

- We're more dependent on data than we realize
  - Most studies use a "per minute" scale to measure cost
- Range from $100,000 to $500,000
- Average $300,000
- Healthcare ≤ $600,000
Impact of Data Loss and Downtime

Items to Consider

• Productivity
  • Patient care
• Employee down time / morale
• Expenses
  • Overtime pay
    • Most temporarily revert back to paper, and then input that data into the EMR system once online

Impact of Data Loss and Downtime

Items to Consider

• IT remediation and reserve resources
• Revenue
  • Reimbursement issues
  • Missed referral opportunity
• Reputation
  • Referral sources
  • Poor patient reviews
  • Lost talent acquisition

Risk Analysis

What business processes are most critical?

• Patient related
• Financial
• Email
• Any application or data that contributes to the operation
  • What data supports those processes?
  • Where is the data located?
Risk Analysis

Operational data
- Thought of as less critical, but how would it impact business?
  - Project plans
  - Research
  - Client relational data
  - Employee information
- Other platforms
  - Voice
  - What did you miss?

Risk Analysis

Your ability to restore and recover data directly corresponds to how susceptible you are to data loss.

Let's talk about RTO and RPO

- Recovery Time Objective (RTO)
  - The length of time a system or core application can be down or offline
- Recovery Point Objective (RPO)
  - The amount of data you can afford to lose

Risk Analysis

More about RTO and RPO

- Requirements may vary
  - At different organizational levels
  - Departments
  - Branch locations
  - For different applications

Having a clear understanding of your RTO and RPO business requirements is the primary guide to your data protection strategy.
# Data Retention

## Who governs retention requirements?

### Medical Records
- **Is it the HIPAA Privacy Rule?**
  - Not Really
- State Laws govern medical record retention

### Time Limit
- **§ 164.316(b)(2)(i)** The Time Limit implementation specification requires covered entities to: "Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later."

## Data Retention

### Who governs retention requirements?
- For supporting documentation as defined by the Privacy Rule?
  - HIPAA preempts State Laws if they have a lesser requirement
- CMS
  - 5 – 10 Years

### Financial
- **IRS**
  - 3 years – general tax returns
  - 6 years to challenge underreported funds
  - 1 to be safe
  - Indefinitely
- **Credit card transactions**
  - 2 years

Your requirements may be longer
Data Protection Methods

Local Protection
- Considerations
  - Risks
    - May be susceptible to an internal viral activity
    - Stored in the same location as servers
    - Non-centralized files
- Considerations
  - Encrypted backup (at rest)
  - Deduplication
  - Compression
  - Backup time frames
  - Isolated backup network
  - Paper

This first line of protection should be a well-oiled machine!

Traditional Backups
- Type
  - Less susceptible to local viral activity
  - Easy to transport
- Data
  - External USB attached, NAS or storage server
  - Faster recovery times
  - Repurposed servers

Snapshots
- SAN
- Hypervisor
- Volume

Data Types
- Transactional Logging
- Databases
- SQL
- Exchange
- Flat vs. Open Files

Offsite
- Offsite Rotation of Local Media
  - Protect from local (data center) isolated events
  - Offsite data is not susceptible to a newly introduced cyber attack
  - Delayed recovery due to the retrieval process
  - Older standard

Offsite Cloud Backup
- Replacing offsite rotation
- Dependent on internet connectivity
Data Protection Methods

Offsite Replication

- Hypervisor
- SAN
- Byte Level

Alternate Sites

- Warm Site
  - Failover system available
  - Not immediately accessible to end-users
  - Requires updated data

- Cold Site
  - Basic infrastructure
  - Typically no server equipment on standby

- Hot Site
  - Available and ready within minutes of an event
  - Based on a real-time replication model

- Active/Active sites – two separate production environments that act as backups for each other

Diversity

- Geographical
  - Weather patterns
  - Avoid overlapping natural or environmental risks
  - Understand the risks of too much distance
Data Protection Methods

Alternate Sites

- Diversity
  - Services
    - Internet Providers
    - Power Companies

- Regulatory Requirements
  - Does the alternate site comply?

Balance the cost of the supporting infrastructure and the complexities of a real-world scenario.

Data Protection Methods

Test, Test, Test

Two primary components:
- The failover/recovery system must meet your RTO requirements
  - RTO also deals with accessibility
  - Users have to be able to access the system
  - This is often overlooked
- It must be functional in that the recoverable data meets your RPO requirements

Don’t wait for a crisis to test your ability to recover data.

Components of a Business Continuity Plan

- Leadership Contacts
  - Decision makers
- Risk Assessment and Business Impact Analysis
- Recovery and Response Procedures

- Recovery Team
  - IT personnel
- Response Team
  - Communications to employees, customers, vendors
Components of a Business Continuity Plan

- Key Personnel Roles
- Notification List
- Logging / Tracking Procedures
- Training Process
- Testing Procedures
- Documented results

Online Resources and Tools

- hhs.gov
  - HIPAA for Professionals: https://www.hhs.gov/hipaa/
- Ready.gov
- SANS Institute
  - Main - https://www.sans.org/
- CMS
- Internet Storm Center: https://isc.sans.edu/
- NIST (National Institute of Standards and Technology)
- Computer Emergency Readiness Team (CERT)
  - US-CERT : https://www.us-cert.gov/

Q&A

Thank you very much.