comportsecure
POWER OF PROTECTION

Disaster Recovery Best Practices for Healthcare & Commercial Organizations

ComportSecure Delivers Best In Class Disaster Recovery

Table of Contents

Disaster Recovery Best Practices

INTRODUCTION

We are in a digital age, and with its benefits there are also challenges. Security breaches, data loss, data corruption, weather-related incidents and acts of terrorism plague nearly every organization and industry.

Governments have instituted increasing numbers of controls to prevent and mitigate risks, in the form of regulations and audits such as SOX, FINRA, and PCI in the financial industry and HIPAA, HITECH and PCI in the medical industry. Organizations are required to comply with these and other government mandates, to protect the privacy of their customers and patients and to ensure that critical data is available to the organization and clinicians sufficient to carry on in the event of business disruption or disaster.

The introduction of electronic medical records (EMR's) improves access and sharing of medical information, the quality of patient care, and lowers costs through efficiency gains. But these advantages create additional responsibilities to manage and protect Protected Health Information (PHI), against theft, loss or disruption.

The following guidelines represent industry best practices for disaster mitigation and recovery. These guidelines are equally relevant to financial, healthcare, and other organizations.

Cloud backup as a service (baas) and disaster recovery as a service (draas)

Most organizations currently handle Disaster Recovery (DR) within their internal IT infrastructure, using tapes and other physical media. However, in the last several years, improvements in cloud security, plus the increase in the amount of data that must be stored and protected, have led many organizations to consider using the cloud for some aspects of Disaster Recovery. Several of the main reasons to consider Cloud Services are:

1) Compliancy – SOC II, PCI or HIPAA

Moving to the cloud with a provider that is compliant and knowledgeable in the requirements of the healthcare, financial and other industries makes it easier to ensure that your organization is maintaining compliance with current and emerging regulations

2) Improved Recovery Objectives

Moving to the cloud with a provider that is compliant and knowledgeable in the requirements of the your organization is maintaining compliance with current and emerging regulations.

3) Rapid and Flexible Deployment

An established cloud (DRaaS and BaaS) services vendor provides fast and flexible resources. They are your partner, providing flexible, secure solutions expeditiously, which otherwise might take an organization several months plus capital expenditures and additional operational overhead.

Theoretically, the solution can be tailored to the organization's current and/or near future backup or DR requirements "on-demand" or close to that. The solution could take on many different aspects - Storage, Compute, NOC and seats with the choice of utilizing all or a subset of the services.

4) Reduced IT Operational Costs

Using cloud services, the organization can rely on a partner that is expert in the technical aspects of Disaster Recovery and delivers on your requirements for increased performance, security, storage space, cost requirements, etc. The organization reduces its IT operational costs and enables its IT staff to focus on initiatives that enhance user experience, improve patient care or better support the lines of business.

BEST PRACTICES

Cloud services (IaaS, BaaS or DraaS) offer many benefits for Disaster Recovery, and cloud-based technology can be more secure against data breaches and losses than an organization's own data center. There are several options for moving DR into cloud; many industries including healthcare have additional requirements around data protection and recovery objectives. Arriving at a proper solution requires a formal approach to selecting and validating how each option satisfies your specific requirements.

The following process steps can be used to assess the organization's readiness, determine the best deployment option, and plan the steps required to achieve its goals.

1) Current DR Environment Assessment

The best way to start planning for a DR strategy that adequately safeguards PHI and other critical or sensitive data is through an IT readiness and security assessment. This helps determine the current state of readiness, exposing issues and gaps and documenting a list areas to be improved.

Assess the risk to the organization if any of the critical applications become unavailable. When making this analysis, compare local recovery versus remote recovery options. By nature, remote recovery will extend RTO unless the environment is protected by replication technology versus data backups.

A Thorough Risk Assessment Includes:

Steps include:

- Identify all critical applications
- Calculate the business or clinical risk for each application if it becomes unavailable
- Calculate the impact, in financial terms, for each application if it becomes unavailable
- Document backup and protection for each critical application
- Determine recovery time for recover each application under the current DR strategy
- Determine the desired RTO and RPO for each application
- Compare the desired RTO/RPO targets to the current state, to determine the exposure gap
- Document readiness of downtime procedures, including training and testing
- Is the organization implementing the 3-2-1 Rule
  - 3 backup copies)
  - 2 (backup onto 2 different media)
  - 1 (1 backup copy offsite)

IT DR Performance

Assess the performance and efficiency of the current backup and recovery system, to identify bottlenecks and determine improvement strategies.

First and foremost, ensure that:

- Data is backing up within the expected timeframe
- IT organization is meeting operational-level agreements (OLAs)
- RTO/RPOs are established per application, with the recovery plan monitored to meet or exceed these objectives

Backup Quality

Assess the file systems and databases to determine if data is at risk. First and foremost, focus on:

- Tracking backup success and failure rates
- Tracking and resolving failed backup jobs
- Ensuring backups are recoverable through testing
- Checking that recovery capabilities are granular to the file level
- Ensuring that data is protected "at rest" encrypted on the current storage medium or target

Restore Capabilities

Assess the current DR plans to determine whether the right processes and capabilities are in place to restore user/business data and all sensitive data such as PHI in the event of a disaster. Focus areas to include:

- Ensure that a formal recovery plan is in place, including the switch from downtime procedures back to information systems and the needed resynchronization
- Test DR systems and processes on a regular basis through live tests and simulated scenarios
- Analyze operational recovery procedures
- Evaluate data integrity and recoverability readiness, including sequence or restoring and restoring interfaces
- Perform a gap analysis of recovery goals versus capabilities
- Ensure there is redundancy built into the systems
- Identify new applications in the environment and update the organization's risk assessment
- Identify any retired systems and confirm that they have been removed from the DR platform and plan

Other Considerations

- How much effort and time is the IT staff dedicating to backup activities?
- Is there a hardware refresh or other IT capital expenditures on the horizon?
- Is the organization looking to add more storage capacity in the near term?

Once the assessment has been completed, there should be a clear understanding of the current capabilities, the gaps, and the efforts required to increase the efficiency and reliability of the current backup systems and restore procedures.

2) Consequence Analysis

Moving Disaster Recovery operations to the cloud is a process that can be accomplished in several ways. Determining which and when aspects of the current operations should be moved to the cloud can be accomplished with a Consequence Analysis. This is a critical step that helps determine which functions are the most critical for the organization.

Define the costs, benefits and risks associated with moving aspects of DR to the cloud. Ensure that the following requirements and constraints are reviewed:

- Financial/budget
- Resource impact
- Technology
- Business processes
- Compliance
- Security
- Business or Patient care/Clinical
- Innovation/growth
- Other elements that are critical to the organization

This will give the organization a clear understanding of its current state of cloud readiness, and provide a plan to move to the cloud by highlighting:

- DR environments that can be migrated immediately for immediate benefit
- DR environments that can be migrated eventually
- DR environments that currently may not be good candidates for cloud, but could be in the future as the business environment changes

3) Solution Requirements

Having determined which processes are good options for the cloud, then outline the requirements including:

- RTO/RPO targets for specific applications
- Application-specific backup requirements (e.g., MEDITECH, Epic, etc., critical business applications)
- Regulatory requirements that impact cloud services vendors (business associates agreement [BAA], High Trust certification, etc.)
- Assurance that data is protected in motion and at rest
- Expectations around DR testing and remediation such as solution deployment timelines
- IT resource requirements, such as cost/budget requirements

4) Your Appropriate Solution

There are several options available, from a fully inhouse, private cloud solution to a fully-hosted solution and points in between. The appropriate scenario is often a mixed approach, based on the applications. If the goal is:

- To restore a lost file or just one server - Local and/or cloud backups (BaaS) are appropriate solutions
- To protect the data foremost and the application second — Cloud Backup (BaaS) is the appropriate solution.
- Quick recovery of the application to restore function to end users - Cloud Replication (DRaaS) is the appropriate solution.

An option is to maintain control over certain aspects of the current DR strategy, but move others (e.g., Backup) to the cloud immediately.

Some options include:

- **Infrastructure-as-a-Service (IaaS)**: Delivers an infrastructure service that allows the organization information to be housed in a professional, managed infrastructure
- **Backup-as-a-Service (BaaS):** Delivers a complete backup solution at the organization's site that provides failover capability to an off-site cloud data center. The entire process is managed by the provider.
- **Disaster Recovery as a Service (DRaaS):** For critical applications that need maximum protection with short RTO and minimum loss on RPO, replication (as opposed to backups) is the appropriate solution. Replication will continually update data and application state to the cloud, providing the preferred plan for rapid recovery.

5) What to Look For in a Cloud Services Provider

Cloud Services Provider must be able to address the above listed requirements and demonstrate that it:

- Has industry experience and expertise, including compliance, such as HIPAA, High Trust certification and willingness to sign the highest level of BAA that includes the latest HIPAA omnibus rule
- Provides a Tier IV data center environment that is SOC II and III and SAEE 16-certified, as well as HIPAA and PCI compliant
- Guarantees service-level agreements
- Provides set response time levels depending on the organization's risk appetite (emergency, urgent, standard and so on)
- Provides RTO and RPO targets that meet the organization's risk assessment guidelines
- Quickly provisions additional services as necessary
- Provides a proof-of-concept so that the organization can test the solution before committing
- Makes recommendations to maximize the return on your current storage investment
- Demonstrates the ability to encrypt data stored within the cloud; such as full disk encryption, volume and virtual disk encryption, or file/folder encryption

CONCLUSION

From a technical standpoint, an organization needs to ensure that any proposed solution will enable it to support the business objectives outlined above, which requires:

- Backing up and restoring massive amounts of data
- Optimizing bandwidth requirements
- Working within IT budget constraints
- Protecting data at rest, as well as when it moves across facilities
- Selecting the best method for storing and restoring applications and data

Contact ComportSecure Today to Discuss your Disaster Recovery Needs