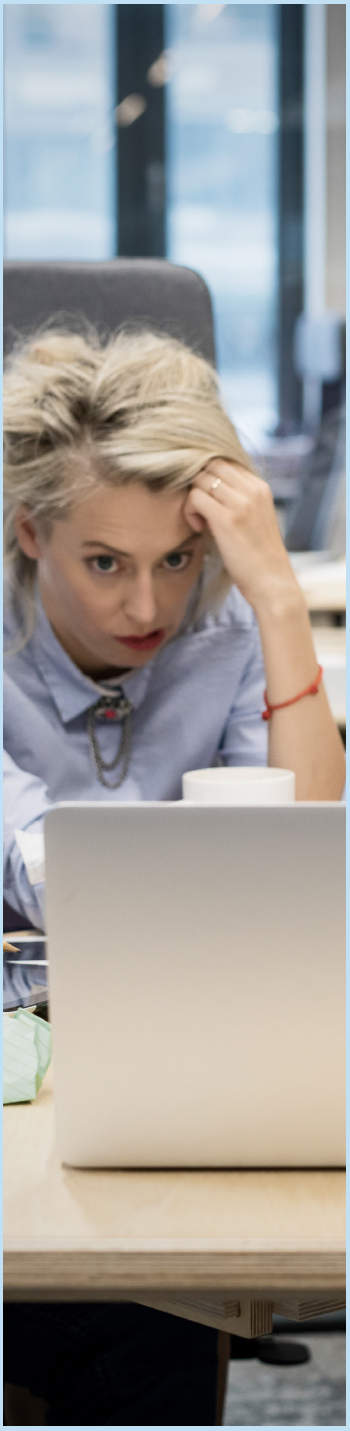
Infosys cobalt

VIEW POINT



IT DISASTER RECOVERY - THINK, APPLY, SUCCEED

Infosys®
Navigate your next

The fast expanding market presence of organizations necessitated the advancement of a robust enterprise IT Disaster Recovery (DR) strategy to safeguard business and organizational assets and prevent failures in the event of a disaster.

The COVID-19 pandemic, infrastructure loss, cyberattacks, natural disasters and operating errors are just a few of the threats organizations face. Meanwhile, the demands of the digital enterprise have raised the complexity, severity and extent of these threats, which may jeopardize the organization's efficiency. As a result, businesses must enhance their ability to react and rebound efficiently in a service interruption.

Over the last few years, cloud and virtualization have completely transformed the way IT organizations manage DR. Organizations must not only find ways to keep performing but also to be more resilient and prepared for the relentless flux in business environments by concentrating on three key elements – redundancy, high availability, and asset replication.

IT DR strategically integrates people, enterprise procedures, infrastructure, resources and governance to ensure that data center failover and failback can occur in a live environment with zero to minimal data loss and business interruption. Replication of applications and entire infrastructure components are automated and technology driven. The subject matter expert must cross-train talent across locations to ensure that resources are available to act during a crisis.

Organizations face these critical challenges–

- Failure to align disaster response, recovery plan and contingency efforts to business specific criteria and results
- Minimal and missing information in reporting all aspects of DR plans, as well as a lack of properly controlled and organized access management
- Absence of complete documentation of interdependencies between applications, infrastructure and critical business processes, which can help formulate a blueprint against which a DR plan can be fully tested and executed
- Poor or selective exercises in DR plans constrain an infrastructure and operations leaders' ability to determine how their organizations can successfully rebuild and resume operations following a disruption

The answer to these challenges lies in designing and validating a DR strategy that includes failover and failback while avoiding data loss by relying on the cloud for redundancy.

The expected business benefits from such a solution include–

- Accomplish the failover and failback of the live system-controlled environment, and achieve the Recovery Time Objective target (RTO).
- Execute database replication and cloud-based recovery technology to simplify data sync during a failover, meeting the Recovery Point Objective RPO).

Achieve best-in-class reliability and availability through the key business processes, infrastructure components, applications and services.

Although danger is inevitable in today's global marketplace, protecting organizational assets in the event of a catastrophe does not happen by default. As disasters with enormous impact become frequent, DR preparation becomes increasingly important.

Planning for Obstacles

Organizations must launch an enterprise-wide DR program in the aftermath of any disaster. This program must be multi-phased and cross-organizational and must provide business procedures for C-level oversight and an IT initiative for DR, to ensure that all infrastructure elements and applications plan to avoid unforeseen incidents.

Today's DR programs of IT utilize a blend of cloud, physical and virtual technologies while ensuring that the operations at the primary data center will failover to the secondary data center, located in different geography if needed.

The mission is to ensure that people are driven by clear and standard best practices in the event of a catastrophe, whether it's a natural disaster, a terrorist attack, or a cyber-attack. Data is continuously being generated, and it's necessary to ensure that no data is lost or corrupted.

In preparation for the worst-case scenario, IT teams must establish criteria for the total downtime and data loss that the organization can handle. While the intent is to avoid business disruption and zero data loss, it is still essential to prepare for that disaster. The IT team defines its criteria for two well-known and established industry protocols –

- RTOis the maximum tolerable amount of time an application or its supporting infrastructure can be down after a breakdown
- RPOis the maximum tolerable duration in which data from the business operations may be lost due to a major event.

These criteria give the IT team a boundary to work with when it comes DR planning.

Business Processes Validation

Simply put, before someone can commit that we have covered all that we have, we must know what we have. The DR readiness phase starts with rigorous documentation, validation and auditing of the underlying IT infrastructure, its associated components, interdependencies and business processes. The lack of legacy procedures or a repository to act as a single source of truth for the underlying IT systems that hold the data is one of the biggest challenges when formulating a DR plan. Organizations are doing their best to simplify the infrastructure and its underlying components as much as possible.

Earlier organizations could define an architecture, design it, and create the end-to-end DR strategy. The main considerations were the application and infrastructure interdependencies that complement business processes. In the absence of consistent DR standards and limited best practices at the start, there was no single point of reference leading to an increase in time spent. However, the consolidation over the past few years into the cloud infrastructure has largely streamlined the infrastructure and helped DR planning.

Today, a deliberate and refined DR program automates failover seamlessly from its primary data center to its secondary data center. The design, definition and development of business procedures allow the CIO to announce a failure and initiate the failover protocol, which is then carefully executed by SMEs from infrastructure and application domains.

The Solution

Cloud-based application environments are highly available and redundant. Today's enterprise consumers should be assured that IT can shield them from major data loss if disaster strikes. By taking a snapshot of the entire infrastructure, the cloud provides continuity. Organizations are also testing application blueprinting to see how it fully automates application recovery. When organizations expand the IT environment and add new applications to the live environment, they also recreate them in their secondary location, also known as the DR site. The DR site is fully open to the users and presents a great advantage for business users. The data is auto replicated or synced continuously or at regular intervals between the primary and secondary site locations.

Disaster Preparedness Testing

Testing for DR takes place in a staged setting that replicates the live environment. Organizations can't shut down the business or take it offline, so a live environment is simulated for all business-critical applications. This is to ensure that IT should be able to complete the failover to live-like environment and levels in much lesser time than the maximum target and with no data loss during RTO testing. During the same testing period, the RPO time should also remain under the planned targeted timeframe.

Only integration components for third-party applications should be reviewed and tested to reduce further complications. However, all suppliers should be subjected to a written DR inspection by the organization.

The risk organizations face cannot be fully mitigated until they have an insight into the third-party's architecture along with their business well-being.

Designing for DR

DR can be divided into cloud infrastructure, virtual infrastructure and physical infrastructure, all of which have failover plans and capabilities. Early DR preparation focused on failover and failback using automation technology, preparation and organizational reform, including mobilizing a new class of "cloud administrators" and improvements to architectural governance, provisioning, release control and monitoring.

The position of IT in a crisis shifts in the cloud age where both failover and failback are automated. IT now concentrates on tracking and escalating problems to the CIO, as well as following the DR instructions to restore normal operations more effectively. The new DR programs were initiated as part of the IT Cloud Transformation program, which accelerated the organization's transition to a Software Defined Data Center and emphasized automation wherever possible. During this process, operational IT also smoothly migrated various mission-critical programs from a virtualized environment to a high-governance cloud platform with limited downtime. Administrators were able to scale vertically and horizontally on demand during training. The end users' ability to provision several real-time, connected business-critical applications in dev/test environments has vastly increased business agility.

With rapid technology advancements, organizations have introduced off-the-shelf solutions from cloud service providers to create a cloud-enabled DR solution through data centers, allowing mission-critical systems to be deployed.

By restoring applications to a given point in time, the established recovery point will defend against data loss. The recovery point should be designed so that it offers continuous data preservation and multiple recovery points using heterogeneous array duplication, which helps IT organizations shorten recovery times. This goes miles ahead as data on the primary and backup servers are kept in line with bidirectional replication. Organizations of mission-critical databases, software, and consumer data would want to ensure that all tools are properly replicated and accessible during a crisis.

Maintaining Continuity

This is where the business continuity (BCP) program comes in with redundancy built in to help businesses brace for disruption. Organizations with multi-country presence have effectively integrated and maintained operations seamlessly. Cross-trained personnel apart from SMEs at multiple locations, are available as backups for each other given that most disasters are regional in nature. IT's DR strategy is only one component of an organization's overall BCP.

Business continuity should be a global initiative for all organizations to help them get back to business as normal after a business disruption. The aim is to keep business running as smoothly as possible both before and during the incident. Documenting critical business processes regularly, updating turnaround plans, and conducting simulations can help organizations be better prepared.

Although IT is responsible for ensuring that the infrastructure is as available as possible and as soon as possible, disaster preparation and restoration to a larger degree is everyone's responsibility across the organization. IT DR under the umbrella of business continuity is a form of literacy that will inevitably be incorporated into all business activities.

In recent years, virtualization and cloud have fully transformed how IT organizations manage their DR. Organizations have not only become adept at keeping the business going but have also become more resilient and open to the ever changing business environments by focusing on redundancy, high availability and replication of assets. A mature and proven strategy is a strategic priority for a steadily growing organization to safeguard its multi-billion-dollar assets and business.

Recommendations

Organizations and their leaders who are responsible for technology, information and resilience risk management should focus on –

- Aligning IT DR preparation with business continuity management, narrowing the spectrum and preparing for failure categories rather than individual situations to improve IT DR services.
- Improving IT disaster recovery network documentation by laying out main protocols, tasks and duties, as well as centrally storing DR schedules for easy access.
- Regularly performing DR exercises, reviewing recovery plans against revised BIA outcomes and revising policies and practices based on the results of DR exercises to enhance DR preparation continuously.

About the Author

Nitin Prasad Yadav
Principal Consultant

Nitin is a Principal Consultant with an eye on increasing business value and enabling user experience through service transformation. Immersed in the IT industry for over 15 years, Nitin works across industry and portfolios, bridging the gap between technology and business through IT Infrastructure services, automation and integration that unlocks true business value. As Principal Consultant, Nitin has worked across the industry verticals, is currently leading Disaster Recovery Management for a Healthcare Client at Infosys and pursuing pointed consulting based on business and strategy management principles as per client needs.

For more information, contact askus@infosys.com

Infosys®
Navigate your next