Top 10 Disaster Recovery Pitfalls

The key to successful disaster recovery is good planning. But with so much at stake for your business, how do you plan with confidence and ensure all stakeholders know what to expect?

The list of variables that can hamper the planning process seems endless: new technologies, old technologies, shifting priorities, data location, compliance, cost, manpower, and much more. As one of the world’s largest network, cloud & managed services, and data center providers, we’ve seen it all, and we know that awareness is the best preparation for the unexpected.

To aid your planning process and ultimately help ensure continuity of your business following a disaster, we want to share some of our experiences. We’ve listed our top 10 most common disaster recovery pitfalls to guide you in developing your own disaster recovery template – along with some helpful hints to stay on course.

Pitfall #1: Not Focusing on Business Needs

Too often companies spend more time assessing technology, data location, space, and vendors than they do gaining a clear understanding of the needs of the business. Before thinking about the technology of disaster recovery, spend time with business leaders and key stakeholders to understand what is most important to them during an extended period of downtime. For sales personnel, access to email or customer relationship management (CRM) systems may be the most important. The finance department may consider a functional financial management system much more important than email. And, customer support staff may be more concerned with the contact center and answering phone calls.

Tip: Understanding the needs of the business will help you establish the right priorities and guide your assessment of disaster recovery technologies.
Pitfall #2: Not Having a Plan

After determining business continuity needs, it is essential to create a disaster recovery plan and obtain buy-in from all stakeholders. The disaster recovery plan must represent all functional areas that the Information Technology (IT) department supports prior to, during, and after a disaster. It must also include all applications, networks, servers, and storage, along with a broad range of “what if” scenarios. In addition, the plan must be kept current. Business priorities often change, and these changes need to be reflected in the plan.

Tip: Keeping your plan current is essential. Business priorities often change, and these changes need to be reflected in the plan.

Pitfall #3: Underestimating Recovery Time

Underestimating recovery time is one of the most costly pitfalls for any business. Unfortunately, this is often realized too late. In an effort to save money, many organizations focus their business continuity efforts on protecting backups of critical business data, storing these in an offsite facility for safekeeping. However, if consideration is not given to recovering this data under a variety of scenarios, problems may arise when disaster strikes.

Take for example a situation where a large geographic area is affected by a major weather event, such as a hurricane. Simply having a copy of the data offsite does not guarantee that you can access the data quickly, acquire the equipment needed to recover the data (tape drives, for example), or restore the data and rebuild application systems fast enough to satisfy the needs of the business. Each of these unknowns must be considered, as they will clearly result in increased downtime and inevitable cost to the business. Understanding the effect of recovery time on the business, and all factors that influence recovery, may prompt you to make different technology and service provider partner choices.

Tip: Understanding the effect of recovery time on the business, and all factors that influence recovery, may prompt you to make different technology and service provider partner choices.
Pitfall #4: Inadequate Testing

A disaster recovery plan is only useful if it works. It is vitally important to test your plan regularly under simulated disaster conditions. This will help ensure you have considered all contingencies and can successfully recover business operations. However, testing a disaster recovery plan can be a challenge for many IT departments. Testing takes time and resources away from day-to-day operations and is often performed at night or on weekends to avoid disrupting production systems. Unless recovery is fully tested at the application level, it is highly likely you will encounter challenges during a real disaster event.

At all times, your focus must be on business applications, with special attention to multi-tier systems that have complex dependencies. These are often the most difficult to recover, and inevitably the most operationally intensive to test. Far too often companies overlook recovery at the application level, checking the box when the server and data have been restored. The results are invariably catastrophic. The goal in testing your disaster recovery plan is to embrace finding and eliminating issues so that all stakeholders have confidence in the plan when a real disaster event happens.

**Tip:** The goal in testing your disaster recovery plan is to embrace finding and eliminating issues so that all stakeholders have confidence in the plan when a real disaster event happens.

Pitfall #5: Unrealistic Recovery Objectives

It’s great to set the bar high for your recovery goals and ensure your business continues with limited disruption during a time of crisis, but it’s also important to understand that your level of redundancy and ability to recover are directly tied to your budget for recovery services. Many organizations have the false expectation that disaster recovery solutions operate like an insurance plan: maximum replacement at a minimal cost. But this is not the case. In general, the more you budget for disaster recovery, the more resilient your applications.

**Tip:** A good practice is to start any disaster recovery planning exercise with the expectation that the cost of a fully redundant system with continuous data replication and near-zero downtime will be equivalent to the amount originally spent to put the system into production. You can then work back from that point in determining your tolerance for downtime against the cost of recovery.
Pitfall #6: Confusing Responsibilities

The fastest way to derail a disaster recovery plan during a real-life event is finding yourself in a situation where key personnel do not understand their role in the recovery process. The plan must clearly identify all stakeholders, and each stakeholder must be aware of their disaster recovery responsibilities. It is essential to involve these personnel in testing the plan.

Tip: Key personnel must also have a designated backup who understands their role in the plan in the event the primary is unable to perform their tasks. It's surprising how many companies commit time, effort, and money to developing a comprehensive disaster recovery plan and then fail at execution time because team members assumed someone else was handling a critical task.

Pitfall #7: Incorrect Measurement of Risk

The definition of a disaster can change from organization to organization, and even from department to department, based on the assessment of risk. Risks come in all shapes and sizes, and it’s essential to ask yourself, what are we trying to protect ourselves from? An unlikely event could be so catastrophic for the organization that it warrants significant investment to avoid the risk, albeit a small risk. Another risk might be commonplace, but have limited financial impact on the organization.

It is important that the disaster recovery plan address the right risks. Cost of downtime is a commonly used metric to measure the impact of an outage to the organization, but it is not an easy figure to calculate. Disaster recovery budgets are often based on cost per hour of downtime and IT teams understandably use best-case estimates when prioritizing recovery. However, these estimates are often overly optimistic.

Tip: To ensure the disaster recovery plan prioritizes the correct applications it is important to have all levels of the business involved in assessing the risk of various disaster scenarios.

Pitfall #8: Unclear Recovery Point and Recovery Time Objectives

Each business application will have a different tolerance for downtime and data loss caused by a disaster. This often reflects the importance of the application to the business. For example, it might be possible to recover data lost from a system that
processes supplier invoices by having suppliers resubmit documentation, but data lost from an online customer order system may be gone forever. An organization’s ability to cope with application downtime and data loss can be measured by recovery time objective (RTO) and recovery point objective (RPO).

RTO measures the amount of downtime the business can withstand, during an application outage, without incurring significant loss. This can be measured in minutes for business critical applications to hours or even days for less important applications. RPO measures the business's tolerance for data loss during application downtime. In the previous example, the online customer order system might have an RPO measured in seconds, whereas applications using data that can be easily recreated may have a much longer RPO.

If the business is to avoid losses following a disaster, applications with smaller RTO and RPO must be recovered faster than those with longer RTO and RPO.

RTO and RPO can be thought of as indicators of priority.

**Tip:** Understanding these metrics is essential for a successful disaster recovery plan. There are many different technologies and techniques to protect against all types of recovery objectives, but the rule of thumb is the lower the RTO and RPO, the higher the cost of a disaster recovery solution.

**Pitfall #9: Focusing on Worst-Case Scenarios**

It is very common for organizations to plan for the worst-case scenario and then be caught out by seemingly trivial events that cause substantial downtime. For example, planning for a catastrophic flood with a warm-site data center in an area outside the flood zone on a separate electrical grid is all very well, but if the primary email server goes down for 24 hours due to a failed upgrade and improper rollback procedures, you have not thought through all possible disaster contingencies.

Many organizations fall victim to being prepared for a cataclysmic event, yet are caught completely off-guard by more common daily disasters that plague IT environments and cause many hours of downtime annually.

**Tip:** In the process of disaster recovery planning, spend the time to refine your definition of a disaster. Setting proper expectations, scope, and definition will keep all stakeholders aligned when these events occur.
Pitfall #10: Separating Budget from the Financial Cost of Downtime

It's impossible to develop a disaster recovery plan that is completely aligned with the needs of the business if a budget is assigned before assessing the financial impact of downtime. Far too often companies set a dollar amount for disaster recovery before evaluating whether the recovery objectives of the business can be met within this amount. This is not an effective approach to disaster recovery.

Tip: As with all financial decisions, determining a budget for business continuity involves making trade-offs. Without a firm understanding of the financial cost of application downtime to the organization, business leaders will be unable to accurately judge the organizational impact of their disaster recovery choices and the risks they are subjecting the organization to.

NTT Communications Recovery as a Service (RaaS)

NTT Communications is a true global company with 130 data centers worldwide, enabling multi-national enterprises to reap the financial and operational benefits from single sourcing their telecom and IT needs. Recovery as a service (RaaS) is a key operational component of our Cloud Vision strategy.

Cloud Recovery Service

NTT Communication’s Cloud Recovery service protects business operations by performing near real-time replication of all operating systems, applications and data to a secure environment in NTT’s Enterprise Cloud. Cloud Recovery is a managed service that provides secure server replication, with automated failover and failback. The service requires no capital investment and can be deployed within hours. Cloud Recovery consists of two offerings that can operate independently or together:

- Cloud-to-Cloud server replication between NTT Communications data centers for organizations currently using NTT services and applications
- Premises-to-Cloud server replication between your private IT infrastructure and an NTT data center.

Data and Application Continuity

NTT Communication’s Cloud Backup is an agent-less architecture that continuously backs up business data to an NTT data center. Cloud Backup supports compression and de-duplication and only copies changed data, reducing network bandwidth requirements. Backup data is hosted on enterprise-class storage in the NTT data
center and is fully encrypted in compliance with Federal Information Processing Standard (FIPS) 140-2. Virtual disaster recovery and application restoration ensure mission critical data and applications are easily recovered in the event of an outage.

**Long-Term Data Archiving**

NTT Communication’s Cloud Archiving service provides a cloud-based archival solution that satisfies mandated regulations for the long-term storage of a business data, files and applications. Cloud Archiving ensures data preservation, integrity, and compliance while dramatically reducing archiving costs.

**About NTT Communications**

NTT Communications provides consultancy, architecture, security, and cloud services to optimize the information and communications technology (ICT) environments of enterprises. These offerings are backed by the company’s worldwide infrastructure, including the leading global tier-1 IP network, Arcstar Universal One™ VPN network reaching 196 countries/regions and 130 secure data centers worldwide.

NTT Communications’ solutions leverage the global resources of the NTT Group: the #1 data center provider in the world. The NTT Group companies include Dimension Data, NTT DOCOMO, NTT DATA and other leading technology companies.

- Comprehensive product and service portfolio spanning data centers, network services, hybrid cloud and pure cloud services
- Offering one-stop enterprise ICT solutions from the NTT portfolio of companies
- Major offices and data centers in key technology locations worldwide for business agility and lowest international latency—including the US West Coast (Silicon Valley) and US East Coast (Northeast Corridor)