IT DISASTER RECOVERY PLANNING EXPLAINED

In today's digital world, technology disruption for even a few hours can result in significant financial consequences to your business. According to Gartner, the average cost of IT downtime is $5,600 per minute. (That's more than $300,000 per hour!) For large organizations, that number tops half a million dollars.

It's no wonder that having a well-designed and effectively maintained disaster recovery plan in place will substantially increase your ability to recover lost data and return to normal operations as quickly as possible.

So, let's look at strategies for developing a disaster recovery plan that will protect your organization.

Business Continuity Planning vs Disaster Recovery Planning:

Business continuity planning (BCP) and disaster recovery planning (DRP) are sometimes used interchangeably. And while they are interconnected, the two are different concepts:

- BCP is the overarching strategy that covers the entire company to ensure that mission-critical functions can continue during and after unforeseen events. Such events could include natural disasters, death or illness of a company executive, a security breach, and more.
- DRP is actually a subset of overall business continuity that helps ensure organizational stability following an impact to IT only. Examples include disruption to servers, desktops, databases, applications and so on.

Goals of disaster recovery

When crafting the right disaster recovery plan for your business, it's important to first assess the goals you'd like the plan to accomplish.

1. Reduce risk

A primary goal of a good disaster recovery plan is to reduce an enterprise's overall risk. Companies should conduct a current risk assessment before forming the plan to understand where vulnerabilities exist that need to be addressed. You can use a number scale to measure each risk level.

2. Resume operations in an emergency

When a disaster occurs, enterprises are working against the clock to push out information and solutions to internal and external customers, resuming operations as quickly as possible.

A disaster recovery plan should offer solutions, for example, using SaaS platforms that are accessible from any location and having redundant data storage and compute abilities.

3. Address owner/investor Concerns

For enterprise businesses, a disaster recovery plan should ease concerns of whoever is at the top of the organization:

- Owners
- Investors
- A board of directors
- Shareholders

Taking inventory of the top concerns from these groups will give you a good idea of high-level corporate liabilities that must be addressed if a plan is to be effective.

4. Update the plan often

A disaster plan should be updated regularly. A good strategy is for the IT department to run routine risk assessments on a schedule and ensure the disaster recovery plan addresses all risks at any given time.

As technology evolves and changes throughout an organization the reaches of that technology must also be considered.

5. Improve disaster response time

A key piece of any disaster recovery plan is ensuring that your IT team and other disaster recovery stakeholders can mobilize quickly and in a coordinated way. You have one shot at having the fastest response deployment possible and getting communications and backups live in the event of an emergency.

To narrow disaster response time, enterprise businesses should routinely test their plan at least

once per year.

6. Comply with industry standards

Most organizations have compliance standards to uphold. Creating an effective DRP will help to reduce the chance of incurring penalties for failure to meet regulatory compliance obligations.

Who creates the Disaster Recovery Plan?

Before you begin mapping out your DRP, it's important to have the right people in place to lead the charge. To this end, establish a disaster recovery plan committee which includes key decision makers from across the entire organization:

- Top management
- IT management
- Human resources
- Finance
- Security
- Vendor management

Collectively, these individuals will be responsible for outlining, implementing, testing and maintaining the disaster recovery plan.

Disaster Recovery Guide: The Contingencies

Here are some key things to consider when approaching your disaster recovery strategy. It's important to note that these are universal principles that should then be tailored to your organization's unique needs and requirements.

1. Ensure Your Plan Can Stand Up to Threats

The initial stages of planning should include risk assessment that includes an analysis of all potential threats and how your enterprise should react to them if they occur. This could include planning for things events like cyberattacks, outages, or natural disasters.

Prioritize your threats by likelihood and give special attention to events that wield the most risk and higher likelihood, for instance, things like a cyberattack may take precedence since they do sometimes occur and come with high enterprise risks.

2. Prioritize Operations with Business Impact Studies

In the face of an unforeseen catastrophic event, IT will be phased with prioritizing which business operations need to be restored first.

To do this, a company must conduct a business impact study of all mission-critical operations to determine the order in which they must be restored. This should be done in conjunction with your risk assessment as outlined in the previous step.

Once you know the likelihood of an event occurring and the expected impact, you can plot these inputs on a risk matrix. Determining a response to each high risk-high impact event in the matrix

should be the focus of your DRP strategy.

3. Take Inventory of Technology

A critical procedural step is that IT should routinely take inventory of all technology -- both hardware and software. As this inventory is updated, so should the disaster recovery plan.

4. Think Beyond Technology

IT departments tend to get lost in planning to restore operations based on their technology platforms, and sometimes forget to prioritize what to do with people and processes.

In a true emergency situation, there will need to be a plan in place for what employees and customers should expect. More on this point in step 7 below.

5. Understand Your Enterprise Tolerance for Downtime

Does your organization how much server downtime you could afford? If not, you should. As a starting point, define the enterprise tolerance for downtime by determining recovery point objectives and recovery time objectives, RPOs and RTOs, as they are sometimes referred.

6. Establish a Plan for Communication

One of the primary motivations of a disaster plan should be to establish communication quickly. This is critical to an effective plan. Consider who needs to be in the know right away and the best way to reach them. Large organizations might wish to establish a mass notification system which will send texts or other messages to personal email addresses if the corporate email system is down. A communication tree is always a good idea as the team works to re-establish cloud systems that allow for communication and collaborative efforts.

7. Plan for Backups

A thorough DRP will define backup work locations and offer redundancy that allows platform users to operate as though there was no disaster. When planning for backups, there are few things to consider:

- Do we need a backup location for employees to collaborate or should they work from home?
- If working from home, are secure access points established?
- Do we need to house data in a backup location or is this something that can be accomplished with SaaS technology?
- What enterprise redundancy needs are there?

Determining the answers to these questions can help you create a full picture of what your backup capabilities should be.

8. Include Disaster Recovery in SLAs

If you work with vendors, how to operate in the event of an emergency should be a basic part of your service level agreement (SLA) with the third-party organization.

9. Consider DRaaS

In an age of SaaS, Disaster Recovery-as-a-Service is a promising option for businesses who don't have the resources to have additional leases or technology required for disaster recovery, in house. DRaaS has many benefits:

- Reduced disaster recovery cost
- Increased simplicity
- Reduced IT resources required
- Maximum efficiency

Template for a Disaster Recovery Plan

By this stage, you know the risks you're planning for, your mission-critical functions, and the methods you need to implement to recover those systems. Now it's time to put it all together in your disaster recovery playbook. This is your roadmap to implementation.

Keep in mind the language used throughout and the importance of explaining assumptions since the DRP document will be viewed by other key players that don't have an IT background but who still need to be able to understand the steps involved.

Gartner has outlined an established method for disaster recovery planning, which you can read about here. The basic categories of your disaster recovery plan should include:

- Initial Analysis
- Introduction or Summary
- Document Outline
- Overview of the Plan
- Overview of the Infrastructure
- Plan Contingency Phases
- Plan Procedures

Final thoughts

If your organization hasn't created a disaster recovery plan or hasn't made it a priority to maintain or improve upon it, then time is of the essence. No business can afford to have an ineffective response to unforeseen circumstances, and once a disaster occurs it's too late. A disaster recovery plan can be the difference between the survival of your business or becoming another statistic.

To avoid costly delays in service, plan your disaster strategy by thinking about goals, performing necessary audits, planning for contingencies and partnering with a third-party vendor, if needed.

Additional resources

For more on disaster planning, check out the BMC Business of IT Blog and these articles:

- The Basics of Business Continuity Management (BCM)
- Disaster Recovery for the Cloud
- What Is GRC? Governance, Risk & Compliance Explained