Acronis

How to Develop an Effective IT Disaster Recovery Plan

A good IT disaster recovery plan will help your company recover lost data and accelerate your organization's return to normal business operations. It will also ensure a disaster will not trigger a major business disruption and adverse financial consequences.

Table of Contents

Introduction

Businesses rely heavily on technology and technology disruption for a few days or even a few hours can result in significant financial loss. According to an ITIC[1] survey, over 95 percent of large enterprises with more than 1,000 employees say that a single hour of downtime costs their company **over $100,000** per year on average.

According to another study by Emerson Network Power and Ponemon Institute[2], the average cost of data center downtime was **$7,908 a minute** in 2013 — or **$690,204** per outage. In addition, 91 percent of data centers experienced an unplanned outage over a 24-month period.

If your company is small to mid-size and does not have a sizeable data center, your organization can be at an even greater risk. According to the Institute for Business and Home Safety[3], an estimated **25 percent of businesses** do not reopen following a major disaster.

If you do not have a disaster recovery plan in place, your company can be a statistic.

Your ability to develop a comprehensive plan to prepare for potential disasters will minimize disruptions and help you maintain normal business operations.

This white paper steps you through the entire IT disaster recovery planning process — from risk assessment to implementation, testing, and ongoing maintenance. We will address topics such as:

- Why you need a disaster recovery (DR) plan.
- What a disaster recovery plan is and how it is different from a business continuity plan.
- The process for creating a successful plan.
- What you need to include in an effective disaster recovery plan.
- How to avoid five common disaster recovery mistakes.

Protect your organization — and your job — with an effective disaster recovery plan.

[1] - "2013-2014 Technology Trends and Deployment Survey," ITIC, http://itic-corp.com/blog/2013/07/one-hour-of-downtime-costs-100k-for-95-of-enterprises

[2] - "Understanding the Cost of Data Center Downtime," Emerson Network Power and Ponemon Institute, http://www.emersonnetworkpower.com/documentation/en-us/brands/liebert/documents/white papers/data-center-uptime_24661-r05-11.pdf

[3] - "Emergency Preparedness," U.S. Small Business Administration, http://www.sba.gov/content/disaster-planning

IT Disaster Recovery vs. Business Continuity

A business continuity plan is a roadmap that "describes the processes and procedures an organization must put in place to ensure that mission-critical functions can continue during and after a disaster.[4] A business continuity plan not only comes into play during times of disaster, but also when other unforeseen events occur such as a major security breach, illness or death of a company executive, pandemic, civil unrest, etc.

A disaster recovery plan is a sub-component of your business continuity plan. It outlines the process, policies, and procedures to prepare for recovery and continuation of the business and infrastructure operations in the event of a power outage, equipment failure, fire, flood, or other disruptive incident.

An IT disaster recovery plan is a major sub-component of your business continuity plan and disaster recovery plan. It is a roadmap that defines the steps to continue IT operations and resume IT systems, including the network, servers, desktops, databases, applications, and any other component of the IT infrastructure.

Your disaster recovery plan should include the following steps:

- Establish a planning group
- Perform a risk assessment and prepare an inventory of IT assets
- Establish priorities
- Develop recovery strategies
- Develop documentation, verification criteria, and procedures
- Test the plan
- Implement the plan
- Maintain the IT infrastructure

Your plan should address all aspects of your infrastructure and provide a step-by-step response process.

[4] - http://searchstorage.techtarget.com/definition/Business-Continuity-and-Disaster-Recovery-BCDR

Every Organization Needs an IT DR Plan

Disasters come unannounced — which is why it is important to get an IT DR plan in place as soon as possible. A fully functioning plan will help you minimize risk exposure, reduce disruption, and ensure economic stability. It will also reduce insurance premiums and potential liability. Most importantly, a well-executed plan can save your organization thousands — even hundreds of thousands — of dollars in the event of a disaster.

To determine how much a disaster can cost your organization, consider the cost of system downtime — the impact on employee productivity, the loss of billable hours, missed sales from a down e-commerce website, penalties for failure to meet regulatory compliance obligations. Data is a valuable asset — customer data; financial, human resource, and R&D documents; and emails are all irreplaceable. Each document represents minutes or hours of work, and retrieving it is essential. In a worst-case scenario, your disaster recovery plan may save your company.

The IT DR Planning Process

Here are the steps you should take when planning for disaster recovery. This process can help ensure organizational stability during and after a disaster.

1. **Establish a planning committee.** Contact key members from various departments and include them in your planning committee. Include decision makers from a variety of departments as well as financial associates, customer service representatives, and IT personnel. Your disaster recovery plan will need to include a list of all group members along with their contact information, roles, and responsibilities in your disaster recovery plan. These individuals must be available in the event of a disaster.

2. **Risk analysis.** Once you establish your disaster recovery planning group, you need to conduct a risk assessment analysis and audit.

   a. Inventory all job titles, office equipment, applications, systems, servers, and software.
   b. Identify the critical needs of your organization. Decide which applications and systems are mission critical, critical, essential, and non-critical.
   c. Assess the probability and impact a disaster can have on these applications and systems. You must consider not just environmental disasters like hurricanes and fires but man-made threats such as virus attacks, infrastructure failure, and employee error (including accidental data deletions).
   d. You might also want to include a business impact analysis (BIA). The purpose of a BIA is to establish recovery time objectives (RTOs) and recovery point objectives (RPOs) for every critical activity within the organization.

3. **Establish priorities for applications and systems.** Now that you have determined the mission-critical applications and systems, you need to prioritize them. Ask yourself the following questions:

   a. How much data can your organization afford to lose?
   b. How long can you go without this data?
   c. How current must the recovered data be?
   d. What needs to be stored onsite and what needs to be stored offsite?
   e. What is an acceptable level of risk?
   f. What is the cost of downtime to your business?
   g. What are the costs of reconstructing this data?
   h. What is the cost per hour of server downtime, including staffing costs?
   i. What does your business insurance cover with regard to replacing lost data?
   j. What is the cost of outsourcing disaster recovery?

Throughout this exercise, your goal is to limit the risk of additional losses and disruption.

4. **Develop recovery strategies.** ISO/IEC 27031, the global standard for IT disaster recovery states, “Strategies should define the approaches to implement the required resilience so that the principles of incident prevention, detection, response, recovery, and restoration are put in place.” When developing your strategies, consider all aspects of your organization, including budget, resources, suppliers, physical facilities, human constraints, technological constraints, regulatory obligations, and risks. Develop strategies for both automatic and manual procedures.

5. **Document your plan.** Once you have completed your risk analysis, established priorities, and developed the necessary disaster recovery strategies, it is time to document this information. Define the rules, processes, and disciplines needed to ensure that your organization's critical business processes will continue to function if there is a failure.

6. **Test your plan.** Set explicit test objectives and success criteria, including your RTO and RPO. Test all functionality, including the recovery of data, failover, access to remote data, and stress testing. Document all verification criteria and procedures within your plan.

7. **Implement your plan.** Share your plan with employees from each department of your organization and be sure to store at least one copy offsite. Sharing the plan ensures that it can be easily located in the event of a disaster. Record all recipients, dates, and locations.

8. **Maintain your plan.** The maintenance of your disaster recovery plan is critical to the success of an actual recovery. Be sure to update your plan to include all changes to facilities, vendors, equipment, applications, software, backup procedures, budget, and personnel (including updated contact information and skill sets). Review the plan annually or semi-annually in conjunction with IT DR testing exercises.

What to Include in Your Plan

The following is an outline for a disaster recovery plan. Every plan is unique, but this sample plan includes the essential information you need to make your plan a success.

1. **Introduction.** Begin your disaster recovery plan with an objective statement, summary, and details about the scope of the plan. Include any assumptions and the criteria for invoking the plan. Specify who created the plan, who approved the plan, and who is authorized to activate the plan.

2. **Roles and responsibilities.** List all disaster recovery team members, including those responsible for operations, networking, and facilities. Be sure to include:

   a. Contact information
   b. The role each plays in a disaster
   c. Job responsibilities
   d. Spending limits (for example, how much money each team member is authorized to spend on equipment)
   e. Any other limits to authority

   It is a good policy to include police and public safety numbers as well.

3. **Other contact information.** Make a list of primary and secondary contact information for all:

    a. Hardware
    b. Operating systems
    c. Software applications and databases
    d. Communications
    e. Facilities
    f. Vendors

4. **Incident response.** Document the plan for assessing site damage and the initial steps in the disaster recovery procedure. Describe all:

    a. Key indicators for minor damage, major damage, and catastrophic damage
    b. Procedures for notifying team members
    c. First steps and standard emergency procedures for all team members

5. **Plan activation.** List the procedures for operating in contingency mode:

    a. Define the criteria for launching the plan, including minimum requirements
    b. Define process descriptions and instructions for all team members
    c. Determine categories for vital records

6. **Return to normal operating mode.** Outline the criteria and procedures for returning to normal operating mode including procedures:

    a. To procure replacement equipment and supplies as required
    b. To restore and/or restart systems as required
    c. To check system functions and results
    d. For notifying personnel to return to normal operating mode

7. **Document history.** Record all of the document dates and revisions for your disaster recovery plan. Be sure to include the name and job title of the person or group of people who revised the plan and also the name and job title of the person who approved all of the revisions.

8. **Procedures.** Once the plan is activated, disaster recovery team members should take the materials assigned to them and proceed with the response and recovery activities that are specified in the plans. The more detailed your plan is, the more likely the affected IT asset will be recovered and returned to normal operation. Include all relevant recovery information and procedures obtained from system vendors. Check with your vendors while developing your plan to see what they have in terms of emergency documentation.

9. **Testing.** Document all testing and include dates and resources that will be managing and performing the testing. You should exercise your DR plan annually or bi-annually.

10. **Appendixes.** You should supplement your disaster recovery plan with your organization's most important documents, including:

    a. Inventory and report forms
    b. Maintenance forms
    c. Hardware lists and serial numbers
    d. Software lists and license numbers
    e. Contact list for vendors
    f. Contact list for staff with home and work numbers
    g. Contact list for other interfacing departments
    h. Network schematic diagrams
    i. Equipment room floor grid diagrams
    j. Contract and maintenance agreements
    k. Special operating instructions for sensitive equipment
    l. Cell phone inventory and agreements
    m. Test scenarios
    n. Insurance policies
    o. Leases and facility information
    p. Equipment purchases
    q. Inventory records
    r. Personnel files
    s. Facility maps
    t. Hazardous material storage details

    Include all of these documents as supporting appendixes to your plan.

Avoid These Common Disaster Recovery Mistakes

Recovering from a disaster is never easy but with the right plan, you can restore your systems — and peace of mind — with as few missteps as possible. Avoiding these five common mistakes will help to make your disaster recovery solution a success.

1. **SAN to SAN Replication.** Replicating data from one location to another is only one function of an effective disaster recovery solution. Be sure to take the following considerations into account as well:

    a. Virtualization environments
    b. Application-specific agents
    c. Snapshot storage requirements
    d. Server activation and documentation
    e. Backup and recovery

2. **Remote Colocation/Location Choice.** Choosing a disaster recovery location is critical to the success of any DR project. When choosing a location, make sure it is not too close to your production site and is capable of remote activation in the event of an emergency. Not all facilities are the same, so check to make sure that your facility is in line with all governance, risk, and compliance standards. For example, facilities should be SSAE 16 SOC Type II certified in the United States and ISO/IEC 24762 certified in the United Kingdom.

3. **Hardware/Software Drift.** Your disaster recovery site represents a working replica of your production environment and as such, you need to maintain it on an ongoing basis. Be sure to keep software licenses, patch levels, and upgrades in sync. If you decide to use old hardware, be sure to calculate the extra maintenance costs required to keep the DR hardware up to date and in parallel with your production site

4. **Failed Testing.** Designing a disaster recovery testing scenario can be a project in itself. If your test fails, you need extra time to analyze the failure and design a solution so be sure to take that into account. Evaluate these costs when deciding whether to create your DR solution in-house, or outsource it to a disaster recovery provider.

5. **Underestimating Resources.** Even if you have talented IT staff and enough resources to execute a disaster recovery plan, will these resources be available when needed? Careful planning and frequent meetings help ensure that your resources will be available in the event of a disaster.

Conclusion

A disaster recovery plan can make the difference between bankruptcy and the survival of your organization. Consider the myriad of reasons why it is important to have a DR plan in place: minimizing lost sales, loss revenue and disruptions to operations; limiting legal liability; lowering insurance premiums; and protecting the assets of your organization. Creating a disaster recovery plan is the first step toward protecting your company from natural and man-made disasters.

Useful Links

Acronis Website
Acronis Disaster Recovery Service
Case Study: Bristows LLC
Case Study: Davis Wright Tremaine LLP

About Acronis

Acronis sets the standard for new generation data protection through its backup, disaster recovery, and secure access solutions. Powered by the AnyData Engine and set apart by its image technology, Acronis delivers easy, complete, and safe backups of all files, applications, and OS across any environment — virtual, physical, cloud, and mobile.

Founded in 2003, Acronis protects the data of over 5 million consumers and 300,000 businesses in over 130 countries. With its more than 100 patents, Acronis' products were named best product of the year by Network Computing, TechTarget, and IT Professional and cover a range of features, including migration, cloning, and replication.