CREATING A DISASTER RECOVERY PLAN

BROUGHT TO YOU BY ColoCrossing

Table of Contents

Introduction

A Disaster Recovery Plan (DRP) is a procedure that a company follows with an aim of recovering and protecting IT infrastructure in the event of a disaster. In this instance, a disaster can be anything from a natural disaster to a prolonged power outage or data security breach. The concept of having a disaster recovery plan is not new. Most businesses have become dependant on computer systems in some form or another, and many small to mid-sized businesses still do not have a DRP. If they do, they are often woefully outdated or unprepared.

This guide is designed to outline a high level overview of the key necessary steps to create and execute a Disaster Recovery Plan.

Small and mid-sized businesses often cannot afford to survive prolonged operational downtime caused by outages and other natural disasters. ColoCrossing is situated with 8 nationwide datacenters strategically placed in geographically diverse major markets, to help your organization create and execute a tailored Disaster Recovery Plan.

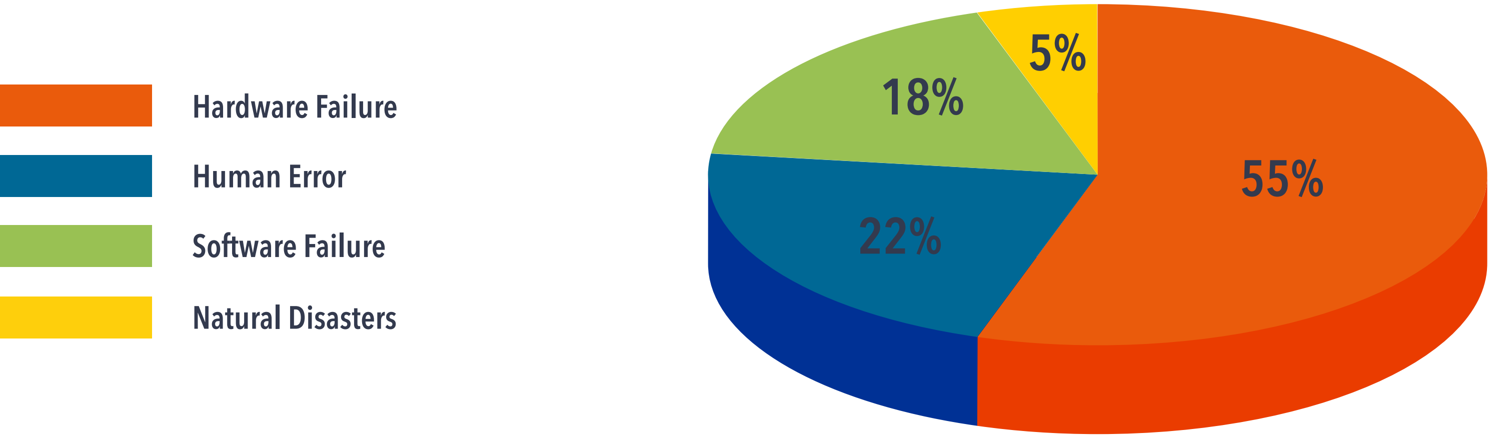
Why Create a DRP?

1 While creating a Disaster Recovery Plan comes with some up-front cost, the long-term benefits are obvious. Reports have shown that every dollar spent on creating a disaster recovery plan saved the company 4 dollars in recovery and response. A recent study by the Ponemon Institute indicates that unexpected downtime can cost some enterprises up to $7,900 per minute.

A sudden and unpredicted event, whether it is a natural disaster, electrical outage or security breach, can greatly affect the day-to-day routine of the company, as well as its bottom line. Every organization should have a Disaster Recovery Plan to enable it to heal quickly and continue offering services to it's customers after the event has occurred.

Downtime is the period of time when mission critical data and IT infrastructure are unavailable or not functional and when companies face downtime, they are cost money. 20% of companies experience a disaster scenario annually. Similarly, in just a year, 80% of these companies will have closed their operations for good largely due to data loss and an inability to recover from extended periods of operational downtime.

IT downtime cost is predicted to be $27.5 billion of revenue loss in North America alone with major companies such as Google and Twitter losing millions of dollars every week. The chart below shows that 55% of downtime is caused by hardware failure along with human error and natural disasters also playing a part.



2

Having a Disaster Recovery Plan is something customers expect. In 2017, it is unacceptable to most customers to not have immediate access to goods and services and any operational downtime can and will cost you their business. Take a moment to consider how quickly your customers might start researching your competition in the event of a prolonged operational downtime. This is a good indication of how little time you have to get your operations back up and running.

In addition to losing business, consider the other lasting effects of prolonged downtime. Your customers do business with you for several reasons, but there is always the matter of trust. Regardless of price, reliability and trust are key factors in a customer's decision to do business with your organization. The moment your products or services become unavailable to a paying customer, the trust a customer places in your company is strained. Restoring those services quickly prevents the trust from being lost and can strengthen the company's reliability.

Planning for Disaster

Creating a Disaster Recovery Plan is specific to the organization it is being planned for.
A Disaster Recovery Plan for a marketing agency in Southern California will undoubtedly look much different than a plan for a SaaS company in Boston. But, there will always be similarities and optimal practices.

Identify Potential Disasters

There are many potential disruptive threats which can occur at any time and affect the normal operations of your organization. It is prudent to consider a wide range of potential threats and the results of those threats becoming a reality.

Ensure that you have identified and mapped out all scenarios and assign a probability grade for each one, regardless of how improbable some may seem.

Potential Disasters

Flood

PROBABILITY RATING: 3
IMPACT RATING: 4

REMEDIAL ACTION:
All critical equipment is located on 1st Floor.

Fire

PROBABILITY RATING: 3
IMPACT RATING: 4

REMEDIAL ACTION:
FM200 suppression system installed in main computer centers. Fire and smoke detectors on all floors.

Electrical Power Failure

PROBABILITY RATING: 3
IMPACT RATING: 4

REMEDIAL ACTION:
Redundant UPS array together with auto standby generator that is tested weekly and remotely monitored 24/7.

Loss of Communications Network Services

PROBABILITY RATING: 3
IMPACT RATING: 4

REMEDIAL ACTION:
Two diversely routed T1 trunks into building. WAN redundancy, voice network resilience.

Tornado

PROBABILITY RATING: 5
IMPACT RATING: 4

REMEDIAL ACTION:
Have critical backups in subterrainean section of facility.

Electrical Storms

PROBABILITY RATING: 5
IMPACT RATING: 4

REMEDIAL ACTION:
Redundant UPS array together with auto standby generator that is tested weekly and remotely monitored 24/7.

Act of Terrorism

PROBABILITY RATING: 5
IMPACT RATING: 4

REMEDIAL ACTION:
Have trained employees on homeland security protocol.

Act of Sabotage

PROBABILITY RATING: 5
IMPACT RATING: 4

REMEDIAL ACTION:
Create standardized process for employee terminations.

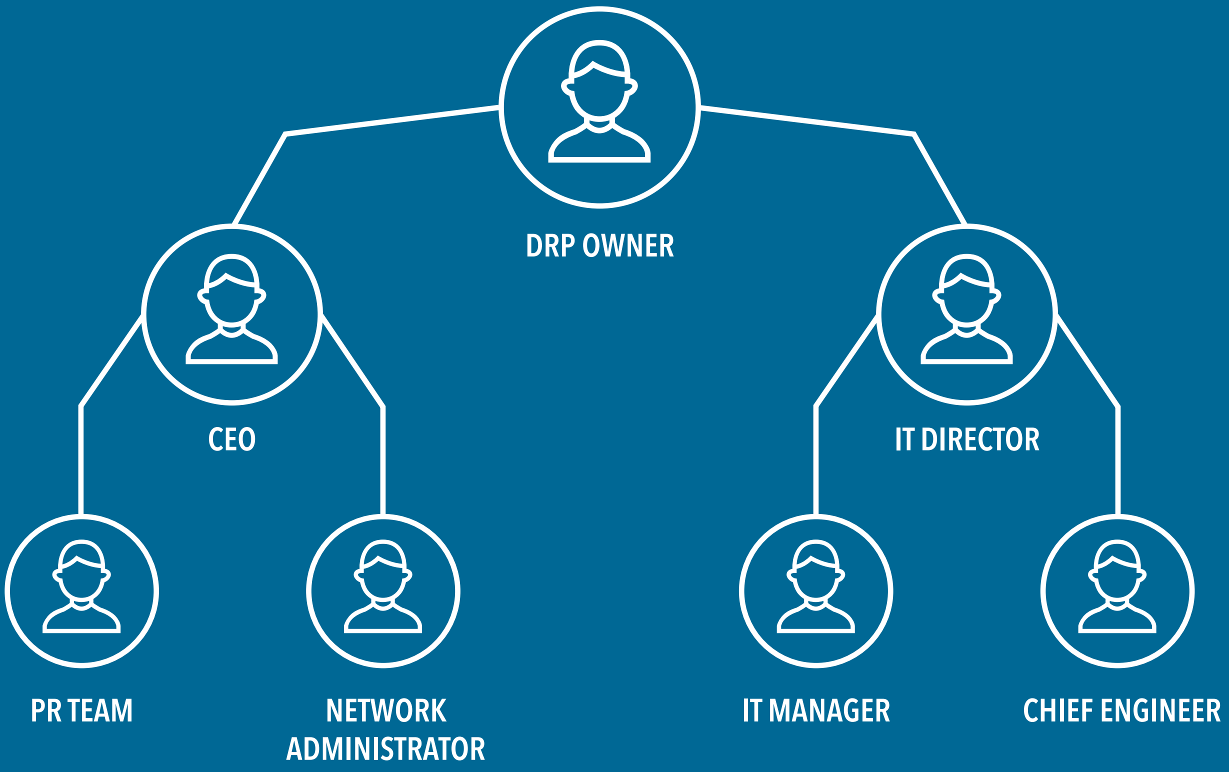
*Sample chart. Data will vary based on location.

Assemble Your Team

After you have identified potential threats, you will need to assemble your DR team. This will include anyone essential to restoring day-to-day operations of the physical location, the IT infrastructure, and anyone that will need to deal with customer service and public relations. The optimal practice is to identify a plan owner. This is not necessarily going to be the highest ranking officer in the company, it can be whomever is most familiar with the day-to-day operations.

Once you have created your team, make sure you have a DRP contact directory.

You are preparing for an unforeseen disaster. Your existing company directory may be inaccessible. The DRP contact directory should be in the form of a calling tree so that your team can be assembled quickly. You will also want to ensure that all employees are aware of this directory and protocol, as you cannot predict who will be identifying the incident. Optimal practice dictates that several copies of this plan should exist in several secure locations in your building, as well as remote copies that will be accessible in the event of a disaster.



Create a Backup Strategy

Your company needs a clear and concise backup strategy regardless of the industry and location. Most companies rely on the 3-2-1 strategy for data backup. What this means is that you should have:

AT LEAST 3 COPIES OF YOUR DATA

TWO OF WHICH ARE ON DIFFERENT MEDIA OR STORAGE DEVICES LOCALLY

A MINIMUM OF ONE OFFSITE BACKUP

For example, you have a file called "clients.csv" on your local hard disk. That is the first copy of the data. You should also have it backed up to an external drive, CD or tape, creating a second copy. You will then need one off-site backup in a data storage facility such as a colocation data center or cloud.

This is a minimum guideline. It is always prudent to create multiple off-site backups that exist in facilities in different geographic locations. During the 2017 Amazon Web Services outage, many companies experienced operational downtime due to storing their data on a single cloud instance. Netflix, on the other hand, had backups in geographically diverse instances, allowing them to recover instantly.

Identify Mission Critical Infrastructure

Depending on your organization, there are going to be several components to your mission-critical infrastructure that need to be identified and listed.

With your internal team, you will need a directory available for all external vendor contacts. This should include your:

PROPERTY MANAGER	TELECOM PROVIDER
SERVER SUPPLIER	HOSTING PROVIDER
INSURANCE PROVIDER	SITE SECURITY
OFF-SITE DATA STORAGE PROVIDERS	HVAC
POWER GENERATOR	CONTACTS FOR OTHER CRITICAL SYSTEMS

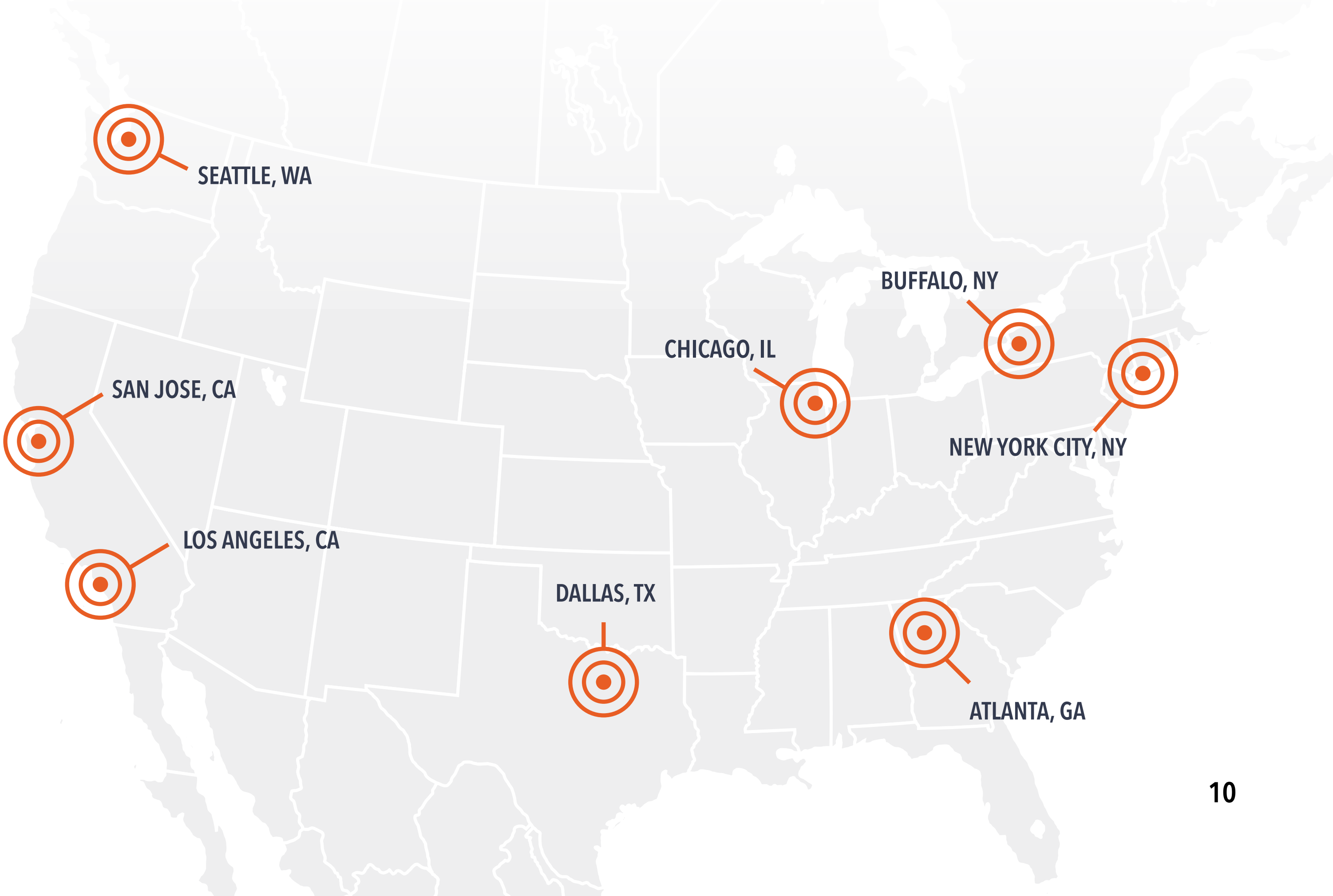
You should identify specific owners for each external contact so that everyone knows who is responsible for what piece of infrastructure.

Select a Disaster Recovery Site

A designated Disaster Recovery Site (DRS) is useful for maintaining business operations while you deal with a disaster scenario. This can be an auxiliary office or a workspace inside a datacenter where your backups exist.

The location of your DRS should be close enough for your essential staff to easily commute to, but in a region that will not be affected by the same disaster, if it is the case of a natural disaster.

It should also be a facility that is equipped with backup power and redundant network capabilities so that you can return to operational status as quickly as possible. Employing a DRS that has facilities and geographically diverse locations ensures that your selection will have a network that is up and running for you to use.



Plan the Execution

You have decided who is needed to execute a DRP, as well as what the mission-critical components of your operations are, now you must decide how to execute your plan. This is where the designated plan owner begins the DRP activation.

Immediate responsibilities of the plan owner are:

1. Respond immediately to a potential disaster and call emergency services if required
2. Assess the extent of the disaster and its impact on the business and datacenter
3. Decide which elements of the DR Plan should be activated
4. Notify and manage the disaster recovery team to maintain vital services and execute the plan to return to normal operations
5. Ensure employees are notified and allocate responsibilities and activities as required

Identify Affected Operations

Since all disasters are different, you will need to assess the situation and determine what operations are affected by the disaster and activate necessary components of the DRP.

It is prudent to consider potential remedies, but in the case of unexpected disasters, spontaneous decisions may be required. In more predictable scenarios, such as a power outage, mapping out a well defined series of rules is optimum.

Keeping records of all affected assets will help with future DR planning, as well as any insurance claims that need to be filed.

Identify Solutions

Work with your Disaster Recovery team to identify solutions to problems created by the disaster.

Map Out a Recovery Timeline

As stated previously, each disaster recovery scenario will require a different level of recovery. A prolonged power outage is more manageable than a complete building loss. Once you have identified the scenario, you should map out a timeline for recovery.

The recovery timeline should be broken down for each piece of infrastructure involved so that realistic expectations can be set for each asset. This will also allow you to activate only portions of the DRP depending on what assets are affected by the disaster.

Return to Operational Status

Implement the necessary processes to reclaim operational status, even if on temporary power, network or within a temporary workstation. Getting operations back will allow you to spend the necessary time to solve the problems created by a disaster while limiting the time it has affected your organization.

Conclusion

Creating a Disaster Recovery Plan is one of the most important things a company can undertake, especially for small and mid-sized businesses. Unfortunately, for many organizations of this size, doing so is not always an easy thing to accomplish. Companies of this size often do not have the resources or personnel to deal with disasters, leaving them vulnerable and unable to compete with larger organizations in the event of a disaster. Fortunately, ColoCrossing can provide the resources and experienced personnel. We will work with your company to not only create a Disaster Recovery Plan tailored specifically to your company, but also execute that plan in the event of a disaster.

We are passionate about helping small businesses compete in today's global economy, and creating a DRP is one way we can help.

If you think your organization can benefit from partnering with us, please do not hesitate to contact us and we will set you up with a dedicated specialist that will take you through all of your options.