Disaster Recovery: Best Practices

Contents

1 Executive Summary

Disasters are inevitable but mostly unpredictable, and they vary in type and magnitude. The best strategy is to have some kind of disaster recovery plan in place, to return to normal after the disaster has struck. For an enterprise, a disaster means abrupt disruption of all or part of its business operations, which may directly result in revenue loss. To minimize disaster losses, it is very important to have a good disaster recovery plan for every business subsystem and operation within an enterprise.

This paper discusses an approach for creating a good disaster recovery plan for a business enterprise. The guidelines are generic in nature, hence they can be applied to any business subsystem within the enterprise.

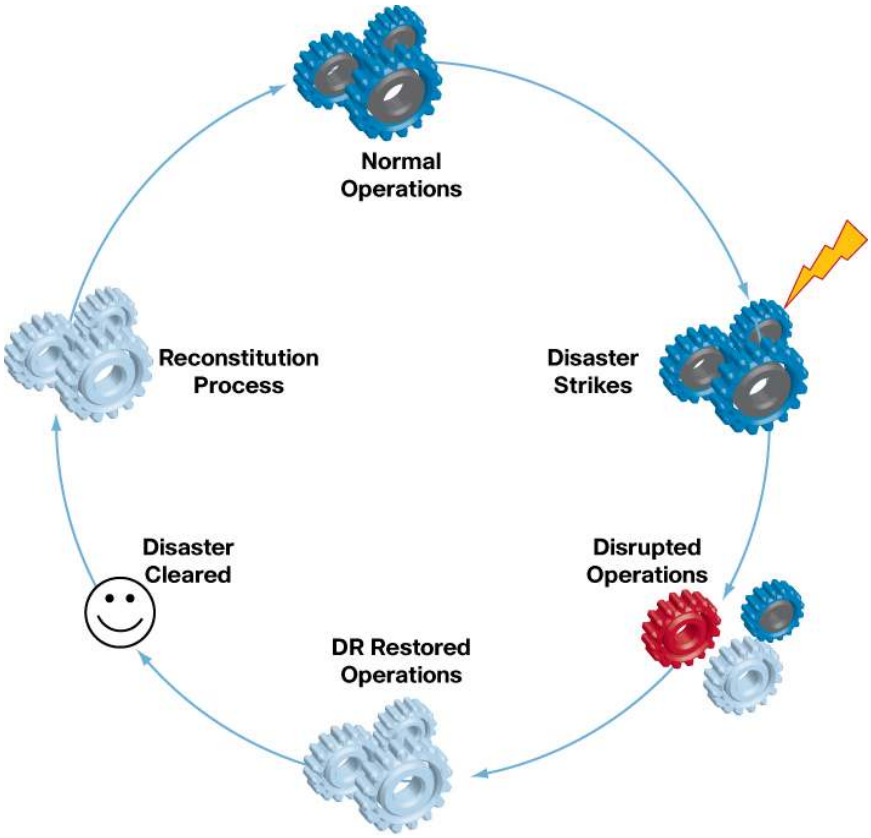
In the IT subsystem, disaster recovery is not the same as high availability. Though both concepts are related to business continuity, high availability is about providing undisrupted continuity of operations whereas disaster recovery involves some amount of downtime, typically measured in days. This paper focuses only on disaster recovery.

Every business disaster has one or more causes and effects. The causes can be natural or human or mechanical in origin, ranging from events such as a tiny hardware or software component's malfunctioning to universally recognized events such as earthquakes, fire, and flood. Effects of disasters range from small interruptions to total business shutdown for days or months, even fatal damage to the business.

The process of preparing a disaster recovery plan begins by identifying these causes and effects, analyzing their likelihood and severity, and ranking them in terms of their business priority. The ultimate results are a formal assessment of risk, a disaster recovery plan that includes all available recovery mechanisms, and a formalized Disaster Recovery Committee that has responsibility for rehearsing, carrying out, and improving the disaster recovery plan.

When a disaster strikes, the normal operations of the enterprise are suspended and replaced with operations spelled out in the disaster recovery plan. Figure 1 depicts the cycle of stages that lead through a disaster back to a state of normalcy.

Figure 1. Enterprise Operations Cycle of Disaster Recovery



It takes the enterprise some time to assess the exact effects of the disaster. Only when these are assessed and the affected systems are identified can a recovery process begin. The disaster recovery system cannot replace the normal working system forever, but only supports it for a short period of time. At the earliest possible time, the disaster recovery process must be decommissioned and the business should return to normalcy.

The disaster recovery plan does not stop at defining the resources or processes that need to be in place to recover from a disaster. The plan should also define how to restore operations to a normal state once the disaster's effects are mitigated. Finally, ongoing procedures for testing and improving the effectiveness of the disaster recovery system are part of a good disaster recovery plan.

In summary, the disaster recovery plan should (1) identify and classify the threats/risks that may lead to disasters, (2) define the resources and processes that ensure business continuity during the disaster, and (3) define the reconstitution mechanism to get the business back to normal from the disaster recovery state, after the effects of the disaster are mitigated. An effective disaster recovery plan plays its role in all stages of the operations as depicted above, and it is continuously improved by disaster recovery mock drills and feedback capture processes.

The second section of this paper explains the methods and procedures involved in the disaster recovery planning process. The third section explains the different phases of disaster recovery. And the fourth section explains what information the disaster recovery plan should contain and how to maintain the disaster recovery plan.

2 Disaster Recovery Planning

This section explains the various procedures/methods involved in planning disaster recovery.

2.1 Identification and Analysis of Disaster Risks/Threats

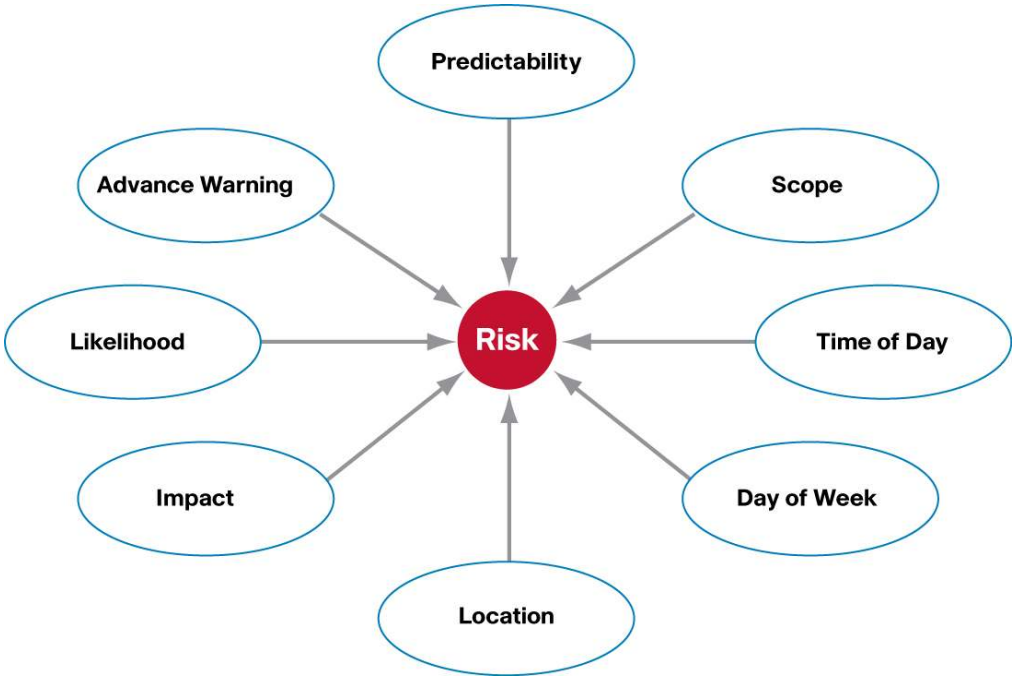
The first step in planning recovery from unexpected disasters is to identify the threats or risks that can bring about disasters by doing risk analysis covering threats to business continuity. Risk analysis (sometimes called business impact analysis) involves evaluating existing physical and environmental security and control systems, and assessing their adequacy with respect to the potential threats.

The risk analysis process begins with a list of the essential functions of the business. This list will set priorities for addressing the risks. Essential functions are those whose interruption would considerably disrupt the operations of the business and may result in financial loss.

These essential functions should be prioritized based on their relative importance to business operations. For example, in the case of a telecom service provider, though both billing operations and CRM/helpdesk operations are essential functions, CRM/helpdesk is less essential than billing. Hence, mitigating the risks that affect billing operations should be given more priority than CRM/helpdesk operations.

While evaluating the risks, it is also useful to consider the attributes of a risk (Figure 2).

Figure 2. Risk Attributes



The scope of a risk is determined by the possible damage, in terms of downtime or cost of lost opportunities. In evaluating a risk, it is essential to keep in mind the options around that risk, such as time of the day or day of the week, that can affect its scope. For example, spilling several gallons of toxic liquid across an assembly line area during working hours is a different situation than the same spill at night or during the weekend. While the time taken and cost to clean up the area are the same in both cases, the first case may require shutting down the assembly line area, which adds downtime cost to this event.

The magnitude of a risk may be different considering the affected component, its location, and the time of occurrence. The effects of a disaster that strikes the entire enterprise are different from the effects of a disaster affecting a specific area, office, or utility within the company.

2.2 Classification of Risks Based on Relative Weights

When evaluating risks, it is recommended to categorize them into different classes to accurately prioritize them. In general, risks can be classified in the following five categories.

2.2.1 External Risks

External risks are those that cannot be associated with a failure within the enterprise. They are very significant in that they are not directly under the control of the organization that faces the damages. External risks can be split into four subcategories:

Natural: These disasters are on top of the list in every disaster recovery plan. Typically they damage a large geographical area. To mitigate the risk of disruption of business operations, a recovery solution should involve disaster recovery facilities in a location away from the affected area. Nowadays most of the meteorological threats can be forecasted, hence the chances to mitigate effects of some natural disasters are considerable. Nevertheless is important to consider documenting the scope of these natural risks in as much detail as possible.

Human caused: These disasters include acts of terrorism, sabotage, virus attacks, operations mistakes, crimes, and so on. These also include the risks resulting from manmade structures. These may be caused by both internal and external persons.

Civil: These risks typically are related to the location of the business facilities. Typical civil risks include labor disputes ending in strikes, communal riots, local political instability, and so on. These again may be internal to the company or external.

Supplier: These risks are tied to the capacity of suppliers to maintain their level of services in a disaster. It is appropriate that a backup supplier pool be maintained in case of emergency.

2.2.2 Facility Risks

Facility risks are risks that affect only local facilities. While evaluating these risks, the following essential utilities and commodities need to be considered.

Electricity: To analyze the power outage risk, it is important to study the frequency of power outage and the duration of each outage. It is also useful to determine how many powers feeds operate within the facility and if necessary make the power system redundant.

Telephones: Telephones are a particularly crucial service during a disaster. A key factor in evaluating risks associated with telephone systems is to study the telephone architecture and determine if any additional infrastructure is required to mitigate the risk of losing the entire telecommunication service during a disaster.

Water: There are certain disaster scenarios where water outages must be considered very seriously, for instance the impact of a water cutoff on computer cooling systems.

Climate Control: Losing the air conditioning or heating system may produce different risks that change with the seasons.

Fire: Many factors affect the risk of fire, for instance the facility's location, its materials, neighboring businesses and structures, and its distance from fire stations. All of these and more must be considered during risk evaluation.

Structural: Structural risks may be related to design flaws, defective material, or poor-quality construction or repairs.

Physical Security: Security risks have gained attention in recent years, and nowadays security is a mandatory 24-hour measure to protect each and every asset of the company from both outsiders and employees. Different secure access and authorization procedures, manual as well as automated ones, are enforced in enterprises. Factors such as workplace violence, bomb threats, trespassing, sabotage, and intellectual property loss are also considered during the security risk analysis.

2.2.3 Data Systems Risks

Data systems risks are those related to the use of shared infrastructure, such as networks, file servers, and software applications that could impact multiple departments. A key objective in analyzing these risks is to identify all single points of failure within the data systems architecture.

Data systems risks can also be due to inappropriate operation processes. Operations that have run for a long period of time on obsolete hardware or software are a major risk given the lack of spares or support. Recovery from this type of failure may be lengthy and expensive due to the need to replace or update software and equipment and retrain personnel.

Data systems risks may be evaluated within the following subcategories:

- Data communication network
- Telecommunication systems and network
- Shared servers
- Virus
- Data backup/storage systems
- Software applications and bugs

2.2.4 Departmental Risks

Departmental risks are the failures within specific departments. These would be events such as a fire within an area where flammable liquids are stored, or a missing door key preventing a specific operation.

An effective departmental risk assessment needs to consider all the critical functions within that department, key operating equipment, and vital records whose absence or loss will compromise operations. Unavailability of skilled personnel also can be a risk. The department should have necessary plans to have skilled backup personnel in place.

2.2.5 Desk-Level Risks

Desk-level risks are all the risks that can happen that would limit or stop the day-to-day personal work of an individual employee. The assessment at this layer may feel a little like an exercise in paranoia. Every process and tool that makes up the personal job must be examined carefully and accounted as essential.

2.3 Building the Risk Assessment

Once the evaluation of the major risk categories is completed, it is time to score and sort all of them, category by category, in terms of their likelihood and impact. The scoring process can be approached by preparing a score sheet, as shown in Table 1, that has the following keys:

- Groups are the subcategories of the main risk category.
- Risks are the individual risks under each group that can affect the business.
- Likelihood is estimated on a scale from 0 to 10, with 0 being not probable and 10 highly probable. The likelihood that something happens should be considered in a long plan period, such as 5 years.
- Impact is estimated on a scale from 0 to 10, with 0 being no impact and 10 being an impact that threatens the company's existence. Impact is highly sensitive to time of day and day of the week.
- Restoration Time is estimated on a scale from 1 to 10. A higher value would mean longer restoration time hence the priority of having a Disaster Recovery mechanism for this risk is higher.

Table 1. Risk Assessment Form

Risk Assessment Form					
External risks					
Date:		Likelihood	Impact	Restoration Time	Score
Grouping	Risk	0 – 10	0 – 10	1 – 10	
Natural disasters					
	Earthquake	1	9	10	90
	Tornado	0	0	10	0
	Severe thunderstorm				0
	Hail	8	3	9	216
	Snow/ice/blizzard	9	5	8	360
Human caused risks					
	Sabotage or act of terror				
	Bridge collapse				
	Water leakage in facility				
Civil issues					
	Riot				
	Labor stoppage and picketing				
Suppliers					
	Power supplier				
	Transportation vendor				

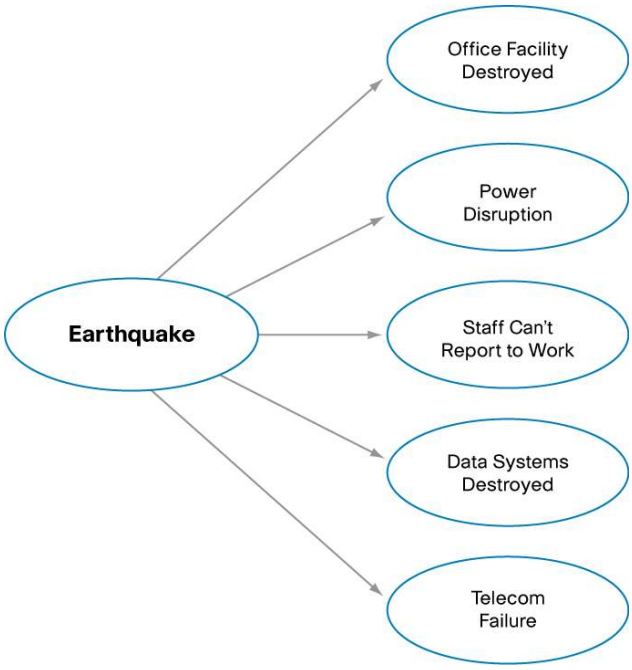
Looking at the above example, multiplying the likelihood time, impact time, and restoration time yields a rough risk analysis score. A zero value within one of the two columns makes the total risk score a zero. Sorting the table in descending order will put the biggest risks to the top, and these are the risks that deserve more attention.

2.4 Determining the Effects of Disasters

Once the disaster risks have been assessed and the decision has been made to cover the most critical risks, the next step is to determine and list the likely effects of each of the disasters. These specific effects are what will need to be covered by the disaster recovery process.

Simple “one cause multiple effects” diagrams (Figure 3) can be used as tools for specifying the effects of each of the disasters.

Figure 3. Disaster Effects Diagram



Note that multiple causes can produce the same effects, and in some cases the effects themselves may be the causes of some other effects.

2.4.1 List of Disaster Affected Entities

The intention of this exercise is to produce a list of entities affected by failure due to disasters, which need to be addressed by the disaster recovery plan. In Figure 3, the entities that fail due to the earthquake disaster are office facility, power system, operations staff, data systems, and telephone system. Table 2 provides a sample mapping of the cause, effects, and affected entities.

Table 2. Determination of Disaster Affected Entities

Risk (Disaster)	Effect of Disaster	Disaster Affected Entity
Earthquake	Office space destroyed	Office space
	Operators cannot report to work	Office staff
	Power disruption	Power
	Data systems destroyed	Data systems
	Desktops destroyed	Desktops and workstations

	Telecom failure	Telephone instruments and network
Power supply cut	Power disruption	Power
	Data systems powered off	Data systems
	Desktops powered off	Desktops/workstations
	Data network down	Network devices and links
	Telecom failure	Telephone instruments and network

It may be noticed that two or more disasters may affect the same entities, and it can be determined which entities are affected most often. The entities with the most appearances in the table have a greater tendency of failure occurrence.

2.4.2 Downtime Tolerance Limits

Once the list of entities that possibly fail due to various types of disasters is prepared, the next step is to determine what is the downtime tolerance limit for each of the entities. This information becomes crucial for preparing the recovery sequence in the disaster recovery plan. The entities with less downtime tolerance limit should be assigned higher priorities for recovery. One metric for evaluating the downtime tolerance limit is the cost of downtime.

2.4.3 Cost of Downtime

The cost of downtime is the main key to calculate the investment needed in a disaster recovery plan. Downtime costs can be divided into tangible and intangible costs.

Tangible costs are those costs that are a consequence of a business interruption, generating loss of revenue and productivity.

Intangible costs include lost opportunities when customers would approach competitors, loss of reputation, and similar factors.

2.4.4 Interdependencies

How the disaster affected entities depend upon each other is crucial information for preparing the recovery sequence in the disaster recovery plan. For example, having the data systems restored has a dependency on the restoration of power.

2.5 Evaluation of Disaster Recovery Mechanisms

Once the list of affected entities is prepared and each entity's business criticality and failure tendency is assessed, it is time to analyze various recovery methods available for each entity and determine the best suitable recovery method for each. This step defines the resources employed in recovery and the process of recovery. Some of the typical entities are data systems, power, data network, and telephone systems. For each of these there are one or more recovery mechanisms in practice in the industry.

In the case of data systems, for example, the recovery mechanism usually involves having the critical data systems replicated somewhere else in the network and putting them online with the latest backed up data available. For less critical data systems, there may be an option to have spare server hardware, and if required these servers could be configured with the required application. Depending on the data system, there may be options of autorecovery or manual recovery, and the cost and recovery time factors of each mechanism vary.

In the case of power, options such as multiple power suppliers or having alternate sources of power such as diesel generators may be suitable. In certain cases, new mechanisms may need to be devised.

Considering multiple options and variations of disaster recovery mechanisms available, it is necessary to carefully evaluate the best suitable recovery mechanism for an affected entity in a particular organization. The main factors that need to be considered are:

- Cost of deployment, maintenance, and operation
- Recovery time
- Ease of recovery activation and operation

2.6 Disaster Recovery Committee

Disaster recovery operations and procedures should be governed by a central committee. This committee should have representation from all the different company agencies with a role in the disaster recovery process, typically management, finance, IT (multiple technology leads), electrical department, security department, human resources, vendor management, and so on.

The Disaster Recovery Committee creates the disaster recovery plan and maintains it. During a disaster, this committee ensures that there is proper coordination between different agencies and that the recovery processes are executed successfully and in proper sequence.

The Disaster Recovery Committee should be authorized and responsible for:

- Creating and maintaining the disaster recovery plan
- Detecting and announcing disaster events within the company
- Activating the disaster recovery plan
- Executing the disaster recovery plan
- Monitoring the disaster situation continuously and returning operations to normal at the earliest feasible time
- Restoring normal operations and shutting down disaster recovery operations
- Continuously improving the disaster recovery plan by conducting periodic mock trials and incorporating lessons learned into the plan after an actual disaster

The roles, responsibilities, and reporting hierarchy of different committee members should be clearly defined both during normal operations and in the case of a disaster emergency. Backup members should also be designated in case of the primary member's unavailability.

Note that not all the members of the Disaster Recovery Committee may actively participate in the actual disaster recovery. But several key members of the committee, such as the operations manager, operations coordinator, and the respective operations team leads, will always actively participate.

3 Disaster Recovery Phases

Disaster recovery happens in the following sequential phases:

1. Activation Phase: In this phase, the disaster effects are assessed and announced.
2. Execution Phase: In this phase, the actual procedures to recover each of the disaster affected entities are executed. Business operations are restored on the recovery system.

3. Reconstitution Phase: In this phase the original system is restored and execution phase procedures are stopped.

3.1 Activation Phase

A disruption or emergency may happen with or without notice. A hurricane affecting a specific geographic area, or a virus spread expected on a certain date are examples of disasters with advance notice. However, there may be no warning of the burst of a water pipe or a human criminal act.

Quick and precise detection of a disaster event and having an appropriate communication plan are the key for reducing the effects of the incoming emergency; in some cases it may give enough time to allow system personnel to implement actions gracefully, thus reducing the impact of the disaster.

The Disaster Recovery Committee is responsible for launching the activation phase. It should be well informed about the geographical, political, social, and environmental events that may pose threats to the company's business operations. It should have trusted information sources in the different agencies to forestall false alarms or overreactions to hoaxes.

The activation phase involves:

- Notification procedures
- Damage assessment
- Disaster recovery activation planning

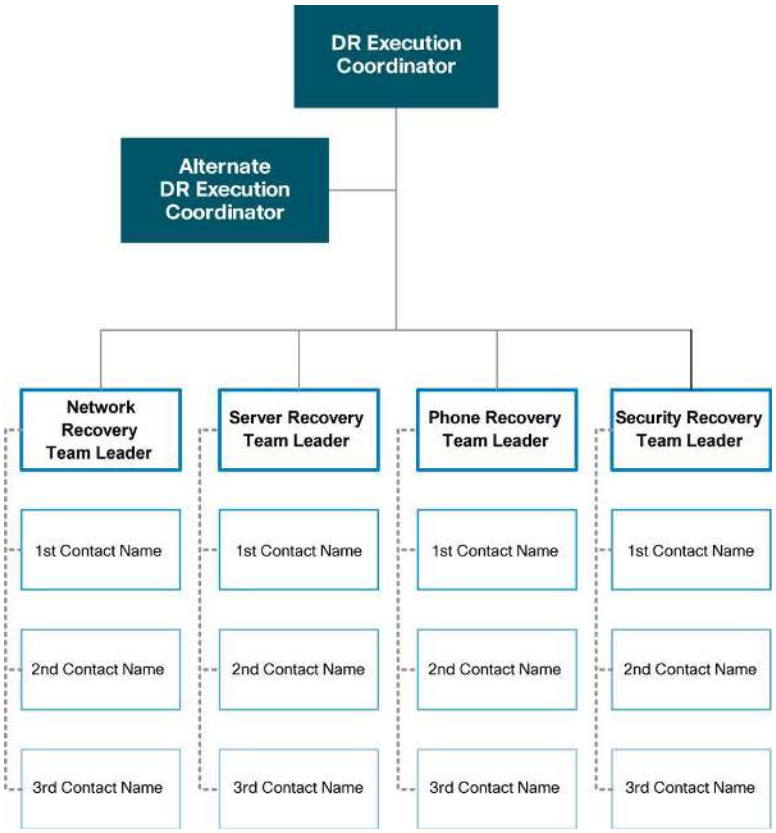
3.1.1 Notification Procedures

The notification procedure defines the primary measures taken as soon as a disruption or emergency has been detected or definitely predicted. At the end of this phase, recovery staff will be ready to execute contingency actions to restore system functions on a temporary basis. Procedures should contain the process to alert recovery personnel during business and nonbusiness hours. After the disaster detection, a notification should be sent to the damage assessment team, so that they can assess the real damage occurred and implement subsequent actions.

Notification can take place by telephone, pager, e-mail, or cell phone. A notification policy must describe procedures to be followed when specific personnel cannot be contacted. Notification procedures should be documented clearly in the contingency plan.

A general notification technique is a call tree (Figure 4). The call tree should document primary and alternate contact methods and should include procedures to be followed if an individual cannot be contacted.

Figure 4. Call Tree Chart



Staff to be alerted should be unmistakably identified in the contact list in the plan. This list should classify personnel by their role, name, and contact information (home, work, and pager numbers, e-mail addresses, and home addresses). If disrupted systems have interconnection with external organizations, a point of contact should be identified in those organizations.

Notification information may contain the following:

- Nature of the emergency that has occurred or is imminent
- Loss of life or injuries
- Damage estimates
- Response and recovery details
- Where and when to assemble for briefing or further response instructions
- Instructions to prepare for relocation for estimated time period
- Instructions to complete notifications using the call tree (if applicable)

3.1.2 Damage Assessment

To establish how the contingency plan will be executed following a service disruption, it is crucial to evaluate the nature and degree of the damage to the system. This damage evaluation should be done as quickly as conditions permit, with personnel safety given highest priority. Consequently, when possible, the damage assessment team is the first team notified of the incident.

It is worthwhile to prepare damage assessment guidelines for investigating different types of major alarms that may progress to a disaster. An example might be a sudden power outage noticed in a data center facility that has a UPS backup. The investigation may determine whether the power can be restored before the UPS system runs out of battery power, in which case activating the disaster recovery plan is not necessary, or otherwise, in which case the plan may be activated immediately.

Damage assessment procedures vary with each particular emergency; nevertheless, the following may be considered in general:

- Origin of the emergency or disruption
- Potential for additional disruptions or damage
- Area affected by the emergency
- Status of physical infrastructure
- Inventory and functional status of the most important equipment
- Type of damage to equipment
- Items to be replaced
- Estimated time to restore normal services if disaster procedures were not in place

3.1.3 Activation Planning

While it is beneficial to detect a disaster at its earliest stage, putting a disaster recovery process into action for a false alarm may stall normal business operations and result in undue costs. Hence it is very important that disaster recovery be activated only when a thorough damage assessment has been conducted.

The disaster recovery plan should have one or more criteria for activation, which become the primary input for evaluating whether the plan should be activated for each affected system. Also, it should be determined whether activating disaster response will bring systems back on line faster than standard procedures.

Depending on the extent of the damage from the disaster, the entire Disaster Recovery Committee or a part of the committee may do the disaster activation planning. The outcome of this planning, at a minimum, should be:

- List of systems and services that need to be restored
- Their interdependencies and sequence of restoration
- Time estimations for each restoration (documented in the plan)
- Instructions for reporting failures to the team leads
- Plan for communication between teams

Once the disaster activation is planned, the appropriate team leads will notify staff and start their respective activities in sequence as they have been instructed.

3.2 Execution Phase

Recovery operations start just after the disaster recovery plan has been activated, appropriate operations staff have been notified, and appropriate teams have been mobilized. The activities of this phase focus on bringing up the disaster recovery system. Depending on the recovery

strategies defined in the plan, these functions could include temporary manual processing, recovery and operation on an alternate system, or relocation and recovery at an alternate site.

3.2.1 Sequence of Recovery Activities

The recovery procedure reflects priorities previously analyzed during the activation planning phase. For instance, if a server room has been recovered after a disruption, the most critical servers should be restored before other, less critical servers. The procedures should also include instructions to coordinate with other teams when certain situations occur, such as:

- An action is not accomplished within the estimated time frame
- A key step has been completed
- Items must be procured

If a system must be recovered at a different location, specific items related to that service need to be transferred or obtained. Recovery procedures should delegate a team to manage shipment of equipment, data, and vital records. Procedures should explain requirements to package, transport, and purchase materials required to recover the system.

3.2.2 Recovery Procedures

The disaster recovery plan should provide detailed procedures to restore the system or system components. Procedures for IT service damage should address specific actions such as:

- Get authorization to access damaged premises or geographic area
- Notify users associated with the system
- Obtain required office supplies and work space
- Obtain and install required hardware components
- Obtain and load backup media
- Restore critical operating systems and application software
- Restore system data
- Test system functionality including security controls
- Connect system to network or other external systems

To avoid confusion in an emergency situation, the recovery procedures should be documented in a simple step-by-step format, without assuming or omitting any procedural steps.

3.3 Reconstitution Phase

In the reconstitution phase, operations are transferred back to the original facility once it is free from the disaster aftereffects, and execution-phase activities are subsequently shut down. If the original system or facility is unrecoverable, this phase also involves rebuilding. Hence the reconstitution phase may last for a few days to few weeks or even months, depending on the severity of destruction and the site's fitness for restoration. As soon as the facility, whether repaired or replaced, is able to support its normal operations, the services may be moved back. The execution team should continue to be engaged until the restoration and testing are complete.

The following major activities occur in this phase:

- Continuously monitor the site or facility's fitness for reoccupation

- Verify that the site is free from aftereffects of the disaster and that there are no further threats
- Ensure that all needed infrastructure services, such as power, water, telecommunications, security, environmental controls, office equipment, and supplies, are operational
- Install system hardware, software, and firmware
- Establish connectivity between internal and external systems
- Test system operations to ensure full functionality
- Shut down the contingency system
- Terminate contingency operations
- Secure, remove, and relocate all sensitive materials at the contingency site
- Arrange for operations staff to return to the original facility

4 The Disaster Recovery Plan Document

The outcome of the disaster recovery planning process is the disaster recovery plan document. During an emergency, this document will be the primary source of information for disaster recovery procedures.

4.1 Document Contents

The disaster recovery plan document is the only reliable source of information for the disaster recovery during an emergency. It should be very easily readable, with simple and detailed instructions. Following are some of the contents that need to be in this document.

- **Document Information:** The document should include information such as the authors/owners with their contact details, revision history and other document details (name, location, version), references, and the audience of the document. In the document revision history, it is good to have a brief description of the changes made in each version. A table of contents is a must for quick reference, and it is highly recommended that the sections be numbered to the lowest possible level for easy reference purpose. It is also good to give an appropriate confidential status for the document as it contains sensitive information.
- **Purpose:** The purpose of the document must be clearly stated in the introduction, defining the objectives the plan intends to achieve.
- **Scope:** The scope of the plan defines the circumstances under which the plan is invoked and the length of time the procedures defined in the document are in effect. The different failure conditions that lead to invoking the plan should be clearly listed. For example, a system being down for couple of hours may not result in invoking the plan, but a daylong outage may suffice. Similarly, the conditions at the failed system/facility that warrant the reconstitution phase should also be clearly stated.
- **Assumptions:** Any conditions the plan assumes to be present for success should be clearly stated. This may involve listing the dependencies of the plan as well. For example, a certain number of trained personnel may be assumed to be available at the disaster recovery facility. Wherever possible, these dependencies must be accompanied with the appropriate contact details.
- **Exclusions:** Any related disaster activities that the plan does not cover should be stated and any known references mentioned here. For example, the plan may exclude the

dependent power restoration plan, referring instead to the appropriate document and the department contact details. Such information will be useful during the disaster recovery.

- **System Description:** The description of the disaster recovery system should be simple to understand with appropriate figures, workflow charts, and so on. If necessary the descriptions may reference appendices that give more detail. The functions that need to be revived need to be clearly mentioned.
- **Roles and Responsibilities:** The roles of the managerial and technical staff and their responsibilities during the activation, execution, and reconstitution phases should be clearly listed. An organization structure diagram showing the reporting relationships is beneficial. Key roles should have primary and alternate personnel assigned.
- **Contact Details:** Full contact information should be included for all the managerial and technical staff involved in the planning, activation, execution, and reconstitution phases. Contact details both during normal situations and emergency situations should be mentioned. This information is recommended to be added as an appendix to the disaster recovery plan document.
- **Activation Procedures:** The procedures for notification, damage assessment, and activation planning should be outlined. Any topic that needs to be covered in great detail may be added as an appendix.
- **Execution Procedures:** The recovery procedure for each of the components the plan covers should be explained step by step in detail. When there are parallel threads of tasks, it is beneficial to have a flow chart diagram to visualize the dependencies of the tasks. The success and failure criteria of each procedure also should be mentioned as well as instructions on further actions in case of both success and failure.
- **Reconstitution Procedures:** Similar procedures for the reconstitution of the components should be explained in detail. The success and failure criteria and instructions for further actions in case of success and failure should be given.

4.2 Document Maintenance

The disaster recovery plan document needs to be kept up to date with the current organization environment. A plan that is not updated and tested is as bad as not having a plan at all because during emergencies, the document may be misleading. The following are recommended for maintenance of the plan documentation.

- **Periodic Mock Drills:** The disaster recovery plan should be tested from time to time using scheduled mock drills. A drill usually will not affect active operations; however, if it is known that operations will be affected, the drill should be carefully scheduled such that the effect is minimal and is done during a permissible window. These activities should be regarded similarly to regular equipment maintenance activities that require operations downtime. The experience of the mock drill should be updated into the disaster recovery plan document.
- **Experience Capture:** The best testing the document will undergo is when an actual disaster happens, and the lessons learned during the disaster recovery are valuable for improving the plan. Hence the Disaster Recovery Committee should ensure that the experience gets captured as lessons learned and the document gets updated accordingly.

- **Periodic Updates:** Technologies, systems, and facilities that the plan covers may change over time. It is important that the disaster recovery plan document reflect the current information about the components it covers. For this purpose, the Disaster Recovery Committee should ensure that the document is audited periodically (say once every quarter) against the present components in the organization. Another way to achieve this is to ensure that the committee is notified of any change that happens to any system/component in the organization so that the committee may update the document accordingly.

5 Reference

Contingency Planning Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology, byMarianne Swanson, Amy Wohl, Lucinda Pope, Tim Grance, Joan Hash, and Ray Thomas. NIST Special Publication 800-34; available at: http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-453495-00 02/08