Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Introduction to Business Continuity Planning

The purpose of this document is to give an overview of what is Business Continuity Planning and provide some guidance and resources for beginner.

Copyright SANS Institute
Author Retains Full Rights

AD

INTRODUCTION TO BUSINESS CONTINUITY PLANNING

Purpose

The purpose of this document is to give an overview of what is Business Continuity Planning and provide some guidance and resources for beginner.

What is Business Continuity Plan?

According to SANS definition[1]:

> Business Continuity refers to the activities required to keep your organization running during a period of displacement or interruption of normal operation.
>
> Whereas,
>
> Disaster Recovery is the process of rebuilding your operation or infrastructure after the disaster has passed.

According to Business Continuity Institute's Glossary[2]:

"Business continuity plan is A collection of procedures and information which is developed, compiled and maintained in readiness for use in the event of an emergency or disaster."

Why we need Business Continuity Plan?

Disaster might occur anytime, so we must be prepared. Depend on the size and nature of the business, we design a plan to minimize the disruption of disaster and keep our business remain competitive.

Due to the advancement of Information Technology (IT), business nowadays depends heavily on IT. With the emergence of e-business, many businesses can't even survive without operating 24 hours per day and 7 days a week. A single downtime might means disaster to their business.

Therefore the traditional Disaster Recovery Plan (DRP), which focuses on restoring the centralized data center, might not be sufficient. A more comprehensive and rigorous Business Continuity Plan (BCP) is needed to achieve a state of business continuity where critical systems and networks are continuously available.[3]

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

When we need Business Continuity Plan?

We need Business Continuity Plan when there is a disruption to our business such as disaster. The Business Continuity Plan should cover the occurrence of following events:

a) Equipment failure (such as disk crash).
b) Disruption of power supply or telecommunication.
c) Application failure or corruption of database.
d) Human error, sabotage or strike.
e) Malicious Software (Viruses, Worms, Trojan horses) attack.
f) Hacking or other Internet attacks.
g) Social unrest or terrorist attacks.
h) Fire
i) Natural disasters (Flood, Earthquake, Hurricanes)

Who should participate in Business Continuity Planning?

With the shift of IT structure from centralized processing to distributed computing and client/ server technology, the company's data are now located across the enterprise. Therefore it is no longer sufficient to rely on IT department alone in Business Continuity Planning, all executives, managers and employee must participate.[3]

Normally Business Continuity Coordinator or Disaster Recovery Coordinator will responsible for maintaining Business Continuity Plan. However his or her job is not updating the Plan himself or herself alone. His or Her job is to carry out review periodically by distribute relevant parts of the Plan to the owner of the documents and ensure the documents are updated.

Where to carry out Business Continuity Plan during disaster?

Cold Site
An empty facility located offsite with necessary infrastructure ready for installation in the event of a disaster.

Mutual Backup
Two organizations with similar system configuration agreeing to serve as a backup site to each other.

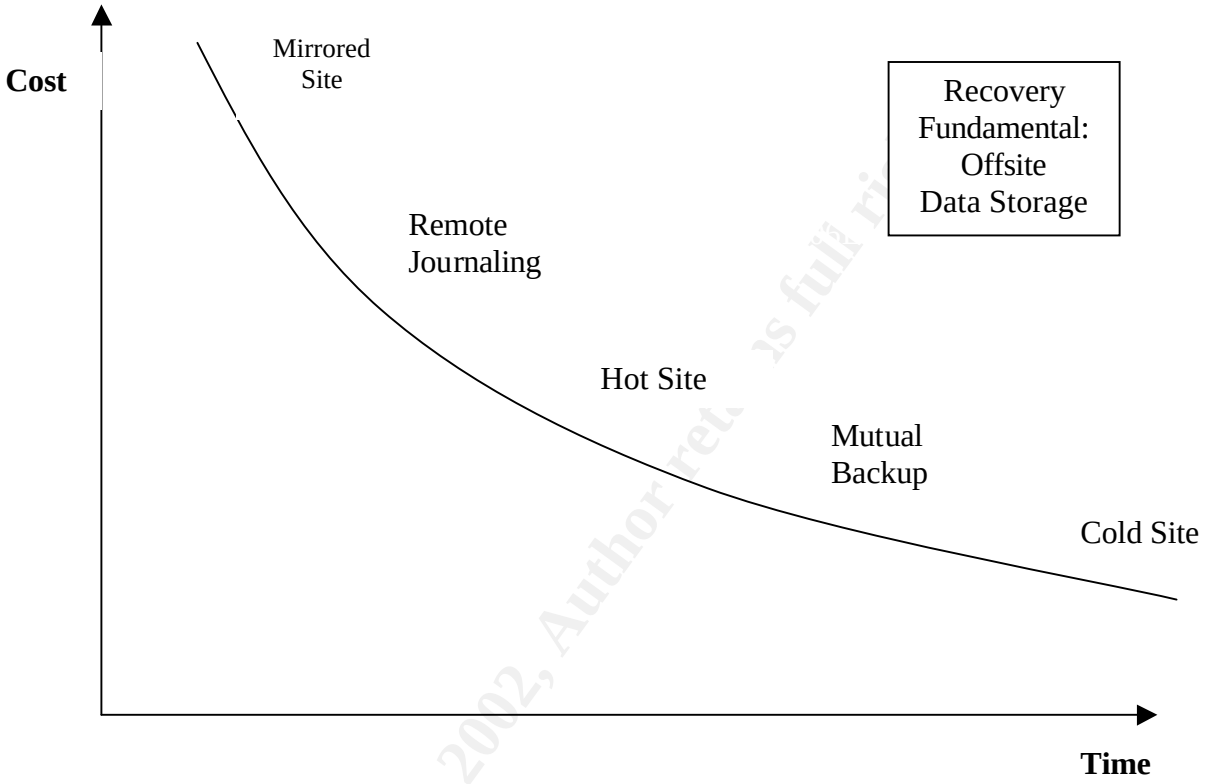
Hot Site
A site with hardware, software and network installed and compatible to production site.

Remote Journaling
Online transmission of transaction data to backup system periodically (normally a few hours) to minimize loss of data and reduce recovery time.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Mirrored Site
A site equips with a system identical to the production system with mirroring facility. Data is mirrored to backup system immediately. Recovery is transparent to users.

Recovery Alternatives[4]



From the diagram, we notice that shorter the recovery time, higher the cost.

<u>Do it yourself or use the facility of service provider</u>

Organization can decide whether to set up the backup center on its own or use the facility provided by of business continuity provider. In making the decision, the organization should consider the following point:

- Availability of facility (floor space).
- Ability to maintain redundant equipment.
- Ability to maintain redundant network capacity.
- Relationships with vendors to provide immediate replacement or assistance.
- Adequacy of funding.
- Availability of skilled personnel.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

How to prepare Business Continuity Plan?

Business Continuity Planning Phases[5]

1. *Project Initiation*
   - Define Business Continuity Objective and Scope of coverage.
   - Establish a Business Continuity Steering Committee.
   - Draw up Business Continuity Policies.

2. *Business Analysis*
   - Perform Risk Analysis and Business Impact Analysis.
   - Consider Alternative Business Continuity Strategies.
   - Carry out Cost-Benefit Analysis and select a Strategy.
   - Develop a Business Continuity Budget.

3. *Design and Development (Designing the Plan)*
   - Set up a Business Recovery Team and assign responsibility to the members.
   - Identify Plan Structure and major components
   - Develop Backup and Recovery Strategies.
   - Develop Scenario to Execute Plan.
   - Develop Escalation, Notification and Plan Activation Criteria.
   - Develop General Plan Administration Policy.

4. *Implementation (Creating the Plan)*
   - Prepare Emergency Response Procedures.
   - Prepare Command Center Activation Procedures.
   - Prepare Detailed Recovery Procedures.
   - Prepare Vendors Contracts and Purchase of Recovery Resources.
   - Ensure everything necessary is in place.
   - Ensure Recovery Team members know their Duties and Responsibilities.

5. *Testing*
   - Exercise Plan based on selected Scenario.
   - Produce Test Report and Evaluate the Result.
   - Provide Training and Awareness to all Personnel.

6. *Maintenance (Updating the Plan)*
   - Review the Plan periodically.
   - Update the Plan with any Changes or Improvement.
   - Distribute the Plan to Recovery Team members.

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Business Analysis is not the only determine factor of Business Continuity strategy, some industry especially those which have public interest (such as financial institution) are required by the regulator to provide certain level of protection to their data. In this case, Statutory Requirement will take precedent over the business decision.

Testing the Plan through the drill with user participation provide a very good training to all the personnel. However, testing should be designed carefully to avoid disruption to Production system. Testing can be designed to test certain functional area only such as network recovery capability or batch processing capability. Procedures and checklists in the Plan should be used during the testing. Testing will highlight the weakness and also status of update of the Plan. Coordinator should conduct testing with management approval at least twice a year to ensure readiness of the Plan.

The Business Continuity Plan normally maintained by Business Continuity Coordinator. Coordinator should identify owners of documents in the Plan. Coordinator should distribute the documents back to their owners periodically (normally half-yearly or yearly depends on the nature of the document) for review and updating. The owners should signoff and return the documents to Coordinator to update into the Plan.

For ease of distribution, Coordinator can put a current copy of the Plan in a server and require authorized keepers of the Plan to make a copy on their own. Owners also required to view the Plan in the server to ensure their documents are updated correctly.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Business Continuity Plan Outline *(simplified based on sample BCP provided by MIT)*[6]

PART I INTRODUCTION

PART II DESIGN OF THE PLAN

1. Overview
   - a Purpose
   - b Assumptions
   - c Development
   - d Maintenance
   - e Testing
2. Organization of Disaster Response and Recovery
   - a Steering Committee
   - b Business Continuity Management Team
   - c Organization Support Teams
   - d Disaster Response
   - e Disaster Detection and Determination
   - f Disaster Notification
3. Initiation of the Business Continuity Plan
   - a Activation of a Site
   - b Dissemination of Public Information
   - c Disaster Recovery Strategy
   - d Emergency Phase
   - e Backup Phase
   - f Recovery Phase
4. Scope of the Business Continuity Plan
   - a Category I - Critical Functions
   - b Category II - Essential Functions
   - c Category III - Necessary Functions
   - d Category IV - Desirable Functions

PART III TEAM DESCRIPTIONS

1. Business Continuity Management Team
2. Organization Support Teams
   - a Damage Assessment/ Salvage Team
   - b Transportation Team
   - c Physical Security Team
   - d Public Information Team
   - e Insurance Team
   - f Telecommunication Team

PART IV RECOVERY PROCEDURES

1. Notification List
   - Contact Information for all the Teams' members.
2. Action Procedures
   - List of Actions to be carried out by each Team.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

There are several commercial software or tools provided by vendors to help planner to develop a professional Business Continuity Plan. Most of the tools can be found at web sites. A few samples of Business Continuity Plan also can be found at Internet for references.

Where to get more information regarding Business Continuity Planning?

DRI International (Web site URL: http://www.dr.org)
DRI International was founded in 1988 to provide a base of common knowledge in contingency planning. It provide following resources:

- Education program
- Professional Certification
- Professional Practices

Disaster Recovery Journal (Web site URL: http://www.drj.com)
The Journal dedicated to Business Continuity since 1987.It provide wide range of resources including the following:

- Magazine
- DR Chat
- Events
- Tools – Sample Plans, DR Glossary, Toolbox
- Vendor Directory

The Business Continuity Institute (Web site URL: http://www.thebci.org)
The Business Continuity Institute was established in 1994 to provide opportunities to obtain guidance and support for business continuity professionals. It provide following resources among others:

- News
- Seminars and Conferences
- BCI Forum
- Glossary
- BCI Standards

Beginners are encouraged to explore themselves to the world of Business Continuity through the websites provided above. The above websites also provide further links to other relevant websites. The practitioners are advice to keep abreast of the Business Continuity world by subscribe to a magazine, join a News group or Forum. The professional practitioner might consider taking the education program and getting the certification.

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Conclusion

With increase of Internet threats and terrorism beside natural disaster and criminals, the business world has become more vulnerable than before. Disaster did happen and it will happen. So be prepared before it is too late.

References

1. Fried, Stephen. "Information Security: The Big Picture - Part IV" Information Security KickStart Highlights, SANS GIAC, 2001.

2. "General Business Continuity Terms" Business Continuity Institute Glossary. URL: http://www.thebci.org/frametrial.html (28 Sep. 2001)

3. "Business Continuity: New risks, new imperatives and a new approach" IBM Executive Brief by IBM Global Services. 1999. Downloadable from URL: http://www-1.ibm.com/services/continuity/recover1.nsf/documents/Business+continuity (28 Sep. 2001)

4. "What is Business Continuity & Recovery Services (BCRS)?" Handout in IBM Security and Availability Seminar. 17 May 2001.

5. "DRI International Business Continuity Planning Model" 15 November 1998. URL: http://www.dr.org/model.htm (21 Aug. 2001)

6. "MIT Business Continuity Plan" 1995. URL: http://web.mit.edu/security/www/pubplan.htm (26 Sep. 2001)

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 20th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced