Focus and Role of Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP)

Version 1.0
29 November 2006

Why Plan?

Companies must plan and be prepared for unexpected events that cause an interruption in business operations. It is critical to the continuity of a business to develop business continuity and disaster recovery plans.

The focus of business continuity planning is to:

1. Minimize interruptions to normal business activity
2. Restore business operations after a disaster or disruptive event occurs
3. Protect the lives of employees
4. Prevent financial losses such as business profits, assets including property, and market share

The Role of a Business Continuity Plan

A Business Continuity Plan (BCP) is a document approved by management. It seeks to ensure that the company can continue operations "business as usual" in the event of a disaster. It is described as a long-term "plan for emergency response, backup operations, and post-disaster recovery to ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation." [1]

The Focus of a Disaster Recovery Plan

The Disaster Recovery Plan (DRP) is a subset of the BCP. It is the company's immediate response to a disruption and focuses on:

- Recovery in predetermined recovery times
- Maintaining the operation of critical business functions
- Identifying resource requirements necessary for recovery
- Identifying alternative recovery strategies

The Role of the DRP

The role of the DRP is to provide staff with a short-term plan of actions to recover the business in the event of a disaster.

A BCP is developed by a team of individuals involved in various aspects of the business. Collectively, the team must understand how the organization conducts its business for the successful development and execution of the plan. The focus of the plan is to provide procedures for staff on how to respond in emergency situations and steps recover as quickly as possible, with the overall goal of ensuring safety to individuals.

What Is a Disruptive Event?

A disruptive event is any act, occurrence, or incident that suspends normal operations. Disruptive events can be intentional or unintentional:

[1] National Computer Security Center

1. **Natural disasters**–Tornado, earthquake, hurricane, fire, landslide, flood, electrical storm, tidal wave
2. **System/technical**–System reboot, erasure of data, system and equipment failure, virus, hacker
3. **Supply systems**–Utility failures such as severed gas or water lines, communication line failures, electrical power outages (blackouts), energy shortage
4. **Human-made/political**–Terrorism, theft, disgruntled worker, arson, labor strike, sabotage, riots, vandalism, crime

Disruptions can be minimized by identifying:

1. Threats, or events/actions that can cause a disruption (human error, natural disasters, viruses)
2. Cost-effective strategies to prevent disruptions, such as a backup generator
3. Insurance to buy to transfer risks
4. Recovery strategies that minimize downtime

The Five Phases of BCP

Several steps must be taken to design an effective BCP:

1. Project Management and Initiation

Obtain management support in developing the BCP. Perform a risk analysis to identify potential outages to critical systems. After approval is obtained from management, appoint a project planner and identify staff to participate in the development **and** execution of the plan. BCP team members should be from various parts of the organization and contain representatives from:

   a. Senior management, CFO
   b. Legal
   c. Business unit
   d. Application and systems support
   e. Data center
   f. Communications
   g. Information security

Develop a project plan similar to traditional project plan phases.

2. Business Impact Analysis

The role of the Business Impact Analysis (BIA) is to identify the impact a disaster would have on critical business functions. This important stage identifies the following:

- Potential threats, the impact of each threat, and its likelihood
- Critical business processes and data systems
- Maximum allowable downtime (MTD) a critical system can incur
- Priorities for critical systems based on MTD
- Internal and external customers to define which business processes are the most important to the organization's survival
- Financial and operational considerations–determine the cost impact if a disruption would occur
- Regulatory requirements–what regulations must the company adhere to and how to sustain them in the event of a disaster
- Organizational reputation–how is market share and the company's reputation impacted if a disaster would occur

3. Recovery Strategies

The recovery phase of the BCP is one of the most important aspects of planning. Recovery strategies are predefined actions approved by management and executed in emergency situations. In this stage, a Disaster Recovery Plan (DRP) is developed. The key element of a recovery strategy is the recovery time of critical business systems in the event of a disaster. Recovery strategies are based on the maximum allowable downtime (MTD) determined in the Business Impact Analysis (BIA).

The recovery process should focus on:

- **Respond** to the disaster.
- **Recover** critical functions.
- **Recover** noncritical functions.
- **Salvage** and repair hardware and software.
- **Return** to the primary site for operations.

The DRP includes various recovery strategies necessary to return the business to operation. Evaluate the cost of each recovery strategy and document that. Plan for contingent operations. Ensure vendor agreements are documented. Obtain management approval for chosen strategies:

- **Business Recovery**–Identification of **critical** systems, data, equipment, materials, office space, and key business support personnel.
- **Facility and Supply Recovery**–Focus on main facility; remote sites; and equipment needed at these sites such as network, servers, telecommunication, and HVAC systems. Include technical documentation, paper, forms and other required supplies, and the transportation of equipment and staff.
- **User Recovery**–

- Document procedures for employees to follow in emergency situations:
  - Team responsibilities–Who does what?
  - Manual processing techniques–Most automated tasks will need to be performed manually.
  - Notification procedures–How are employees notified?
  - Disaster policies–Safety first may be one of the company's policies in the event of a disaster.
- Focus on personnel requirements such as:
  - Vital records storage, such as information on staff including emergency numbers
  - Employee transportation because some employees may need to be picked up from home and taken to the alternative site
  - Desks, computers, and phones for users
  - How employees will access the alternative site

- **Operational Recovery**–
  - Determine the configurations of computer equipment required for recovery:
    - Mainframes, servers, peripherals, LANs, switches, routers, and other data communication equipment
  - Determine alternative strategies for recovery locations based on MTD and acceptable costs. Businesses may opt to secure a facility equipped as follows (listed here highest to lowest cost):
    - Mirror site–No downtime, fully equipped, and staffed with actively running identical processes. Use of redundant technologies such as Redundant Array of Inexpensive Disks (RAID), clustering, and backup power supplies
    - Hot site–Minutes-hours downtime, similar to mirror site except data/staff may be lessened
    - Warm site–Days-weeks downtime, pre-equipped and partially prepared for operations
    - Cold site–Weeks-months downtime, facility with basic HVAC and connections

    Additional location options include:
    - Reciprocal or mutual aid agreements–Use another business's site as an alternative location for recovery.

        - Multiple processing centers–Spread the work to several locations that can handle the businesses operational requirements during recovery.
        - Service bureaus–Contract recovery needs to an offsite service bureau placing the responsibility of having the site ready and available.

- **Software and Data Recovery**–Focus is on the recovery of the data, such as:
    - Back ups and offsite storage–Ensure backups occur at a frequency required by the business for optimum recovery and that backup tapes are stored at an offsite location.
    - Database shadowing–Database information is duplicated by being simultaneously written to another server.
    - Electronic vaulting–Batch process that makes a copy of backup data to an offsite location.
    - Remote journaling–Similar to electronic vaulting except live data transfers are passed to the offsite location allowing full synchronization of both sites.

4. Plan Design and Development

The BCP team prepares and documents a detailed plan for recovery of critical business systems. The combination of the various steps and actions in the design and development phase result in the deliverable of the BCP document. The plan includes both long-term and short-term goals such as recovery plans, employee training, plan maintenance, and testing procedures.

- **Define the scope of the plan**
    a. Identify critical sites, systems, and business processes.
    b. Set priorities for restoration.
    c. Define why the plan is important, i.e. this site runs systems that produce revenues in excess of 2.5 million dollars per day. .
- **Identify potential disasters** that may impact the site and minimum resources needed to recover. Include any assumptions that might impact the success of the plan--for example, the plan includes a key secondary site and assumes that the secondary site was not affected by the disaster. Identify actions that might eliminate risks in advance
- **Define the BCP strategy**–If a disruptive event occurs, what steps are taken to restore critical business functions? Document the procedures to avoid confusion during a time of crisis:
    - Select recovery strategies.
    - identify which vital personnel, systems, and equipment are needed to recover.

- Identify the team's roles and responsibilities.
- Document clear guidance on declaring a disaster:

  Who will declare a disaster?

  Which event is considered a disaster to our business?

  When/at which point/after how much time will a disaster be declared?

  Which method of communication will be used?

  What will be communicated?

  How will the information be cascaded to staff?

  How will communications to external groups such as customers, shareholders, the media, the community, emergency services organizations, etc. be handled?

- **Calculate funding** required to accomplish the long- and short-term goals identified.

5. Testing, Maintenance, Awareness, and Training

The final phase of BCP is testing and maintenance of the BCP, as well as staff training. How will you know that the BCP plan works? It is imperative that the plan made in the plan design and development phase is effective regardless of the disaster, and that it can be executed as designed. Training and awareness programs are required for key staff to ensure that they understand what to do in the event of a disaster.

A. Testing

Five types of BCP testing:

- **Checklist**–Copies of the plan are sent to different department managers and business unit managers for review. This is a simple test and should be used in conjunction with other tests.
- **Structured Walk-through**–Team members and other individuals responsible for recovery meet and walk through the plan step-by-step to identify errors or assumptions.
- **Simulation**-This is a simulation of an actual emergency. Members of the response team act in the same way as if there was a real emergency.
- **Parallel**–This is similar to simulation testing, but the primary site is uninterrupted and critical systems are run in parallel at the alternative and primary sites.
- **Full interruption**–This test involves all facets of the company in a response to an emergency. It mimics a real disaster where all steps are performed to test the plan. Systems are shut down at the primary site and all individuals who would be involved in a real emergency, including

internal and external organizations, participate in the test. This test is the most detailed, time-consuming, and expensive all of these.

B. Plan Maintenance

It is important to establish change management procedures to maintain and make changes to the plan. If changes are required due to testing, reclassification of systems from to critical or noncritical, locations, or personnel changes, a centralized command and control structure is effective for the maintenance of the plan.

C. Awareness and Training

Organizations should design and develop training programs to ensure **each** employee knows what to do in case of an emergency. Periodic awareness programs will allow the company to keep employees interested in the criticality of business continuity.

Appendix

Sources:

CISSP Exam Cram 2, Michael Gregg, Que Publishing 2006.

SANS +S Training Program for the CISSP Certification Exam 414.5 Business Continuity Planning & Law Investigations & Ethics, various authors, The SANS Institute 2006.

The (ISC)^2 CISSP CBK Review Seminar Domain 9 Business Continuity Planning, The International Information System Security Certification Consortium, Pearson Custom Publishing 2006.

Intro to Information Security 309.6 Disaster Recovery and Business Continuity Workshop, Stephen Fried, Fred Kerby, Stephen Northcutt, David Rice, GIAX Prep, The SANS Institute 2004.