Business Continuity Planning and Disaster Recovery Planning

Ed Crowley CISSP

‘05

Topics

- BCP
- Prime BCP elements
- Business Impact Assessment (BIA)
- Three types of backup services
- DR
- Disaster recovery plan process
- Five types of disaster recovery plan tests

BCP/DRP

- Assures viability of organizational digital assets through emergencies and disasters.
  - BCP focuses on viability through routine emergencies.
  - DRP focuses on disaster recovering.

Continuity Disruptive Events

- Concerned with planning for events, either natural or man-made, that may threaten an organization's continuing existence.
- All plans and processes are reactive.

Scope

- BCP process includes:
  - Scope and plan initiation
  - Business Impact Assessment (BIA)
  - Business continuity plan development
- DRP includes:
  - Processes
  - Testing
  - Procedures

Contingency Plans Defined

" A plan for emergency response, backup operations, and post-disaster recovery maintained by an activity as a part of its security program that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation…"

National Computer Security Center, 1988

1997-98 survey >35% of companies have no plans

Business Continuity Planning

- Prevents interruptions to normal business activity
  - Protects critical business processes from man made and natural disasters
- Strategy
  - Minimize disturbances effects
  - Business processes resumption.
- Disruptive Event
  - Any intentional or unintentional security violation that suspends normal operation.

BCP Address

- Staff
- LANs/WANs and their components
- Telecommunications/data links
- Workstations/workspaces
- Applications software
- Data
- Media and records storage

Sample Disruptive Events

- Natural
  - Fire
  - Earthquakes
  - Power Outages
- Man-made
  - Bombings
  - Strikes
  - Communication infrastructure failure

Four BCP Elements

1. Scope and Plan Initiation
2. Business Impact Assessment (BIA)
3. Business Continuity Plan Development
4. Plan Approval and Implementation

Scope and Plan Initiation

- Scope Creation
- Detailed account of work required
- Resource listing
- Defined management practices

Roles and Responsibility

- Senior Management
  - Ultimate responsibility
- Executive Management
  - Initiates project, gives ongoing support and final approval
- BCP Committee
  - Creates, implements, and tests plan.
- Senior Business Unit Management
  - Identifies and prioritizes critical systems
- Functional Business Units
  - Participate in implementation and testing

FCPA 1977

- Foreign Corrupt Practices Act imposes civil and criminal penalties if publicly held organizations fail to maintain adequate controls over their information systems.

Due Diligence

- If a disruptive event causes losses that adherence to base industry standard of due care could have prevented, this is the concept through which stockholders may hold senior managers as well as the board of directors personally responsible.
- Due Diligence then means that the company can demonstrate that it has taken all reasonable steps in protecting its employees.

Due Care

- The standard of "due care" is that level of diligence which a prudent and competent person would exercise under a given set of circumstances.

- http://www.isaca.org/standard/guide14.htm

Comparison

- Due Care
  - Minimum and customary practice of responsible protection of assets that reflects a community or societal norm.
- Due Diligence
  - Prudent management
  - Execution of due care.

Business Impact Assessment

- Documents a disruptive event's impact.
  - Used to create awareness
  - Impacts may be financial or operational.
- Often, a vulnerability assessment is part of the BIA process.

Vulnerability Assessment Produces

- Loss impact analysis
  - Financial
  - Operational
- Critical support areas listing
  - Areas required for business continuity

BIA Primary Goals

- Prioritize Criticality.
  - Critical business unit processes identified and prioritized.
  - Disruptive event's impact evaluated.
- Estimate Maximum Tolerable Downtime (MTD)
    - Down time that business can tolerate and still remain viable.
- Articulate Resource Requirements

BIA Process Steps

1. Gather needed assessment materials
2. Perform vulnerability assessment
3. Analyze compiled information
4. Document results and present recommendations

Gathering Assessment Materials

- Identify which business units are critical to a continuing acceptable level of operations.

Vulnerability Assessment

- Similar to Risk Assessment in that there is:
  - An objective Quantitative (financial) section.
  - A subjective Qualitative (operational) section.
- Differs from RA in that it is smaller.
- Focuses on providing information solely for BCP/DR.

Quantitative Loss Criteria

- Financial losses:
  - Revenue loss, capital expenditure, personal liability.
  - Resolution of contract agreements violation
  - Resolution of regulatory or compliance requirements violation
- Additional operational expenses incurred due to the disruptive event

Qualitative Loss Criteria

- Loss of:
  - Competitive advantage or market share
  - Public confidence or credibility or incurring public embarrassment.
- A critical support area is defined as a business unit or function that must be present to sustain continuity or business processes, maintain life safety, or avoid public relations embarrassment.

Critical Support Areas

- Telecommunications, data communications or information technology
- Physical infrastructure or plant facilities, transportation services.
- Accounting, payroll, transaction processing, customer service, purchasing.

Analysis Phase

The analysis phase includes activities such as:

- Documenting required processes
- Identifying interdependencies
- Determining what an acceptable interruption period would be.

BCP Development

Two steps

1. Define continuity strategy
2. Document continuity strategy

IT Department

- Identifies company's dependencies
  - Internal and external information.
- Should ensure that an organization employs:
  - An adequate data backup and restore process
  - Sufficient physical security mechanisms to preserve vital network and hardware components.
  - Sufficient logical security methodologies
  - Implements adequate system administration including up to date hware, sware, and media inventories

Defining Continuity Strategy

- Includes elements such as:
  - Computing
  - Facilities
  - People
  - Supplies and equipment

BCP Approval and Implementation

- Senior management approval
- Enterprise wide plan awareness
- Plan maintenance (updates)

Disaster Recovery Planning

- Comprehensive action plan dealing with disruptive events.
- Primary objectives
  - Implement critical processes at an alternative site.
  - Return to the primary site and normal processing within a time frame that minimizes the organizational loss.

DRP Goals

- Organized decision methodology for use during a disruptive event.
- Reduce confusion
- Can include
  - Protection from major computer services failure
  - Minimize risk from delays in providing services
  - Through testing and simulation, guarantee standby systems reliability
  - Minimize decision making during a disaster

Disaster Recovery Planning Process

- Development and creation of the recovery plans (similar to the BCP process).
- Two steps
  - Data Processing Continuity Planning
  - Data Recovery Plan Maintenance

Data Processing Continuity Planning

- Most common alternate processing types
  - Mutual aid agreements
    - aka reciprocal agreement
  - Subscription services
  - Multiple centers
  - Service bureaus
  - Other data center backup alternatives

Mutual Aid Agreements

- A mutual aid agreement (sometimes called a reciprocal agreement) is an arrangement with another company that may have similar computing needs.
- As opposed to a hot or warm site, reciprocal arrangements severely limit the responsiveness and support available to the organization during an event.
  - Can be used only for short term outage support.

Subscription Services

- Third party commercial service that provides alternative backup and processing facilities.
- Three basic forms
  - Hot site
  - Warm site
  - Cold site

Hot Site

- A fully configured computer facility with:
  - Electrical power
  - Heating ventilation and air conditioning
  - Functioning file/print servers
  - Workstations.
- Optimal
- Most expensive

Warm Site

- Readily available computer facility with electrical power, HVAC, and computers.
- Applications may not be installed or configured.
- Compared to a hot site:
  - Cheaper
  - More flexible
  - Lower administrative overhead

Cold Site

- Site ready for equipment to be brought in.
- No computer hardware.
- A room with electrical power and HVAC.
  - Computers must be brought on site
  - Communications links may not be ready.

Service Bureaus

- In rare cases, an organization may contract with a service bureau for all alternate backup processing services.

Other Data Center Backup Alternatives

- Rolling/mobile backup sites
- In-house or external supply of hardware replacements
- Prefabricated buildings.

Transaction Redundancy Implementations

- Electric vaulting
  - Offsite transfer of backup data
- Remote journaling
  - Parallel transactions processing on an alternate site
- Database shadowing
  - Live processing of remote journaling
  - Creates more redundancy by duplicating database sets to multiple severs.

Disaster Recovery Plan Maintenance

- For many different reasons, all recovery plans quickly become obsolete.

Disaster Recovery Plan Testing

- A tape backup system cannot be considered working until restoration tests have been conducted…
- Testing:
  - Verifies the recovery procedures accuracy and identifies deficiencies
  - Prepares and trains personnel to execute their emergency duties
  - Verifies the alternate backup site processing capability

Test Document

- Document outlining test scenario must contain:
  - Reasons for the test
  - Test objectives
  - Type of test to be conducted.
- The test's purpose is to find weaknesses in the plan.

Five Disaster Recovery Plan Test Types

- Checklist
  - Individual departments review.
- Structured walk-through
  - Business unit reps meet to walk through the plan
- Simulation
  - Goes to the point of relocating to alternate backup site or enacting recovery procedures

Five Disaster Recovery Plan Test Types

- Parallel
  - Full test of the recovery plan.
- Full-interruption
  - A disaster is replicated to the point of ceasing normal operations.

Elements of Disaster Recovery

- Recovery team
- Salvage team
- Normal operations resumption
- Other recovery issues

Recovery Team

- When a disaster is declared a clearly defined recovery team has the mandate to implement the recovery procedures.

Salvage Team

- A salvage team, separate from the recovery team, returns the primary site to normal processing environmental conditions.
- Has the mandate to quickly and safely:
  - Clean
  - Repair
  - Salvage
  - After the immediate disaster has ended, determine primary processing infrastructure's viability.

Normal Operations Resume

- The steps to resume normal processing operations will be different than the steps in the recovery plan; that is, the least critical work should be brought back first to the primary site.

Other Recovery Issues

- Interfacing with external groups
- Employee relations
- Fraud and crime
- Financial disbursement
- Media relations

External Groups

- Often, the organization may be well equipped to cope with a disaster in relation to its own employees, but overlooks its relationship with external parties such as:
  - Police
  - Fire
  - EMS
  - Utility
  - Press

When is the Disaster Over?

- When all operations have returned to their normal location and function.

Other Recovery Issues

- How does the organization manage its relationship with its employees and their families?
- In major physical disasters, fraud and crime along with vandalism and looting are common.
- Procedures for storing signed, authorized checks off site must be considered in order to facilitate financial reimbursement.
- How does the plan address dealing with the media and with civic officials.

Questions?