Business Continuity Planning
CSH5 Chapter 58
Business Continuity Planning
Michael Miora

Topics
- Basic Concepts
- Defining Goals of BCP
- The BIA
- BIA Matrix Analysis
- Justifying Costs of BCP

Basic Concepts of BCP
- BCP and DRP
- Overview
- Enterprise Risks and Costs
- Types of Disasters
- Recovery Scenarios

Overview
- Increasing dependence on technology
  - Mission-critical systems (production)
  - Development
  - Management
- Business Continuity Planning (BCP)
  - Protecting organizations against consequences of unavailability of such systems
  - Focus on enterprise operations, not just IT
- Must define “fast enough”
  - In each context of the business

BCP and DRP
- Business Continuity Planning
  - Identifying critical functions
  - Developing the critical path for recovery
  - Evaluating costs
  - Gaining management approval
- Disaster Recovery Planning
  - Preparing specific strategies for recovery
  - Defining specific tasks (steps) needed to implement those strategies
  - Testing and revising

Enterprise Risks and Costs
- Fundamental risk is to survival of organization
  - Case of La Ferme St Laurent
  - Clients of Mathema in Montréal in 1980s
  - Failed in 1986 when computer error caused them to stamp milk products with wrong expiry dates

Copyright © 2014 M. E. Kabay
All rights reserved.
Enterprise Risks and Costs (cont’d)

Exhibits are from Michael Miora’s Chapter 42 in CSH4.

Days After Disaster

% of Daily Income

Exhibit 42-1. Fiscal losses caused by disasters.

Types of Disasters (cont’d)

- The specific disaster scenario is not as important as the recovery process and recovery time
- Group disasters into types to facilitate planning
- Break BCPs into modules to activate as appropriate

Types of Disasters

Exhibit 42-2. Disaster Threats

- Accidents
- Equipment Problems
- Arson
- Flood
- Blackout
- Forced Evacuation
- Bank Threat
- Hurricane
- Building Failure
- Ice Storm
- Chemical Spills
- Ice Rainstorm
- Civil Disorders
- Labor Disputes
- Civil Disturbances
- Mechanical Breakage
- Computer Component
- Municipal Services
- Stealage
- Computer Virus
- Postal Service Disruption
- Construction Damage
- Power Loss of Flooding
- Construction Demolition
- Riot
- Data Theft
- Security Breach
- Data Loss
- Strike
- Discharged Employee
- Terrorism
- Drug Abuse
- Tornado
- Forfeiture
- Torn Spots
- Elevator Failure
- Vandalism
- Envelopment
- Wrack
- Environmental Control Failure
- Water

Recovery Scenarios

- Recovery scenarios have 3 phases

Defining Goals of BCP

- Overview
- Scope
- Correlating Objectives to Corporate Missions and Functions
- Validating Goals
- Mapping Goals to Recovery Phases
- Emergency Issues

Topics

- Basic Concepts
- Defining Goals of BCP
- The BIA
- BIA Matrix Analysis
- Justifying Costs of BCP

Copyright © 2014 M. E. Kabay  All rights reserved.
Overview of Setting Goals

- Setting goals a multi-step process
- Define minimum service levels required for acceptable performance
  - Define specific goals for specific sectors
  - Gain approval and support of steering committees of appropriate sector
  - Gain overall approval of upper management
- Goals are defined in business terms not in terms of means and systems
- Process may be iterative

Scope

- Define environment to be protected
  - Who and what are to be included?
  - Will protect specific
    - systems,
    - equipment,
    - procedures,
    - locations, and
    - support capabilities
- Expect to refine and redefine scope during planning process
- May have to define stepwise (phased) implementation plan for BCP

Correlating Objectives to Corporate Missions and Functions

- IT often (usually) develops BCP
  - Systems engineering disciplines help
  - IT infrastructure critically important
  - May already have contacts throughout organization for functional support
- Must expand beyond IT
  - Need business perspective
    - CIO is only one C-level exec
- Much may depend on processes outside scope of IT function
  - Must not overlook non-IT-dependent systems
  - SCM and CRM go beyond automated systems

Corporate Missions and Functions (cont’d)

- Examples of often-overlooked functions
  - Mail room
  - Facilities support
    - Especially important in emergencies and for recovery
  - Security forces
  - Work from 3 main documents
    - Organization chart
    - Corporate phone directory
    - List of corporate operations budget line items

Missions and Functions (cont’d)

- Distinguish between importance of a function
  - To the overall corporate goals
  - To BCP / disaster recovery goals
- Mostly a matter of timeline
  - Determine how long function can be suspended (or running at minimal levels) without harming organization
  - May change depending on circumstances
    - E.g., corporate tax function may be long-term goals at mid-year yet more critical at tax-filing time
- Need top-management sign-off on fundamental goals – affects everything else

Validating Goals
Mapping Goals to Recovery Phases

- Begin with low levels and increase slightly.
- Continue with increasing levels.
- Restore to normal operations.

Exhibit 42.6: Service levels mapped to recovery activities.

Emergency Issues

- Ensure safety of employees and others potentially affected by disaster
  - Health protection (gas masks, hazmat suits, etc. as appropriate)
  - Safety preparedness (fire extinguishers, training, CPR, ...)
  - Shelter & care for employees involved in disaster or in recovery
  - Search & rescue teams
- Effective public relations may keep a problem from becoming a disaster
  - Honest, timely, accurate and controlled release of information

Topics

- Basic Concepts
- Defining Goals of BCP
- The BIA
- BIA Matrix Analysis
- Justifying Costs of BCP

Establishing Scope of BIA

- Inventory equipment & capabilities to be protected or recovered
- Will change over time
- Must be kept up-to-date
- Remember communications infrastructure
- Establish documentation
- Office equipment may also be critical
- Include security systems

Interviews

Exhibit 42.7: The Three Steps of Interviewing

- List All Functions in the Department
- List All Functions by Area
- Dep't Functions

People who do the work are the best sources of information about those functions
- Determine whom to interview
  - List departments
  - Select individual in each dept as 1st interviewee
  - Determine functions within each department
  - Avoid excessive detail
  - Group means into functional goals
    - E.g., specific forms for SEC = "SEC reporting"

Copyright © 2014 M. E. Kabay
All rights reserved.
Interviews (cont’d)

- Goal: develop chart showing relative importance of different functions
- Will be important in determining critical path (timeline) for recovery

Describing Functions

- Must include summary information about each function listed
  - 1 or 2 ¶
  - Reduce confusion
  - Focus discussions
- Use functional matrix as shown below to represent functions

Definition of Departments & Functions

- Survival Days
  - How long can organization survive without this function before significant damage?

Definition of Departments & Functions (cont’d)

- Operational Impact
  - Convert criticality to Operational Impact
  - 4 levels instead of 10
  - Reduces granularity of criticality

The Ranking Factor

- Combines survival time and operational impact
- Low number is most important
- Multiply survival time (days) x operational impact
  - E.g., 1 day survival x op impact critical (1) = 1
  - 10 day survival x op 1 = 10
  - 3 day survival x “some op impact” (3) = 9
Category

- Sort by Ranking Factor in ascending order
- Category groups functions with similar recovery periods

Exhibit 42-13. Category Assignment Curve

Category (cont’d)

BIA Matrix is Heart of BIA

- Basic information needed to
  - Establish recovery requirements
  - Timelines
  - Estimate costs of outages
- Useful in
  - Translating business objectives into BIA objectives

Exhibit 42-14. A Sample BIA Matrix

Listing the Functions Organizationally

Finding Cross-Department Functions

- Emphasize similar functions in different departments
- Titles may differ but functions same or almost
- Especially important to resolve different estimates of parameters (Survival days, criticality, impact, ranking factor...)
- Must adapt to irreconcilable perspectives

Exhibit 42-14. A Sample BIA Matrix
### Cross-Department Functions

<table>
<thead>
<tr>
<th>Department</th>
<th>Functions</th>
<th>Survival Days</th>
<th>Criticality</th>
<th>Ops Impact</th>
<th>Ranking Factor</th>
<th>No. at Home</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corporate Services</td>
<td>Payroll Billing</td>
<td>15</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>I</td>
</tr>
<tr>
<td></td>
<td>Facilities</td>
<td>15</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>II</td>
</tr>
<tr>
<td>Crop Accounting</td>
<td>Cash Management</td>
<td>15</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>II</td>
</tr>
<tr>
<td>Human Resources</td>
<td>IT</td>
<td>15</td>
<td>1</td>
<td>4</td>
<td>4</td>
<td>1</td>
<td>II</td>
</tr>
<tr>
<td>Materials</td>
<td>Production Scheduling</td>
<td>15</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>II</td>
</tr>
<tr>
<td>Customer Service</td>
<td>Data Entry</td>
<td>15</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>II</td>
</tr>
<tr>
<td>OA</td>
<td>Project planning</td>
<td>15</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>II</td>
</tr>
</tbody>
</table>

Exhibit 42-15. Emphasizing Cross Departmental Functions

### Using the Ranking Factor

<table>
<thead>
<tr>
<th>Department</th>
<th>Functions</th>
<th>Survival Days</th>
<th>Criticality</th>
<th>Ops Impact</th>
<th>Ranking Factor</th>
<th>No. at Home</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Human Resources</td>
<td>Risk Management</td>
<td>15</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>II</td>
</tr>
<tr>
<td>Corporate Services</td>
<td>Facilities</td>
<td>15</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>II</td>
</tr>
<tr>
<td>Crop Accounting</td>
<td>Cash Management</td>
<td>15</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>II</td>
</tr>
<tr>
<td>Human Resources</td>
<td>IT</td>
<td>15</td>
<td>1</td>
<td>4</td>
<td>4</td>
<td>1</td>
<td>III</td>
</tr>
<tr>
<td>Materials</td>
<td>Production Scheduling</td>
<td>15</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>II</td>
</tr>
<tr>
<td>Customer Service</td>
<td>Data Entry</td>
<td>15</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>II</td>
</tr>
<tr>
<td>Marketing</td>
<td>P&amp;C</td>
<td>15</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>II</td>
</tr>
<tr>
<td>Human Resources</td>
<td>Risk Management</td>
<td>15</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>II</td>
</tr>
<tr>
<td>Human Resources</td>
<td>CICS</td>
<td>15</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>II</td>
</tr>
</tbody>
</table>

Exhibit 42-16. The Ranking Factor View

### Ranking Factor (cont’d)

Critically important functions that must be restored first.

Exhibit 42-17. Graphing the Three Measures

### Topics

- Basic Concepts
- Defining Goals of BCP
- The BIA
- BIA Matrix Analysis
- Justifying Costs of BCP

### Quantitative Risk Model (QRM)

- Annualized Loss Expectancies
  - ALE = \( \sum p_i c_i \)
  - \( p_i \) is probability of event or strategy \( i \)
  - \( c_i \) is cost (or gain) of event or strategy \( i \)
- E.g., in roulette (gambling game),
  - Probability \( p_i \) of winning \$1 bet on a single number on a roll of wheel is \( 1/38 \) and gain \( c_i \) is 36 times the bet = \$36
  - Losing: \( p_2 = 37/38 \) with \( c_2 = -\$1 \)
  - So ALE for this bet is \( p_1c_1 + p_2c_2 \)
  = 0.0263*36 + 0.9737*(-1) = \( 0.0269 \) per bet

### Problems of the QRM

- Costs depend on level of loss
  - E.g., costs will rise as outage lengthens
  - Complicates calculations
- Most important: exact probabilities difficult to determine
  - Some events have extensive data base
  - Actuaries keep records for insurance companies – fire, flood, etc.
- But IT-related probabilities difficult to find
  - Huge variations in infrastructure, configuration, exposure to threats
  - Operational standards affect vulnerabilities
Generalized Cost Consequence Model (GCC)

- Estimate cost of damage for each function
  - When does the loss begin?
  - What are the monetary consequences?
- Apply cost when appropriate
- Collect costs by category

GCC (cont’d)

- Evaluate total losses day-by-day

Review Questions (1)

1. Distinguish between BCP and DRP
2. Why is BCP important to IT today?
3. What is the advantage of grouping disasters into types in BCP?
4. What are the three phases of recovery scenarios?
5. Why do you need BCP steering committees for different sectors of the organization? Why can’t a BCP expert simply define the goals of the process herself?
6. How does defining the scope of the BCP support the planning process?
7. Why does the IT sector so often get the responsibility for coordinating BCP?

Review Questions (2)

8. What are the 3 main documents recommended by Prof Miora as the basis for identifying key corporate functions?
9. In the description of functions for the functional matrix, what does the criticality score signify?
10. What is the relation between the operational impact score and the criticality score in the functional matrix?
11. In the functional matrix, how is the ranking factor calculated? What is the ranking factor used for?
12. In the functional matrix, what is the relation between the category and the ranking factor? What is the category used for?
13. What’s the benefit of listing functions organizationally in the BIA matrix?

Review Questions (3)

14. How does sorting by ranking factor in the BIA matrix serve BCP needs?
15. A fire-insurance policy costs Megahard Corp $10,000 per year for the Miora Complex on the Northfield Campus to cover the $8,000,000 cost of rebuilding it were it to burn down. Actuaries inform the risk managers at Megahard that the probability of a catastrophic fire is 0.001 per year. Calculate the ALE of the insurance policy and then calculate the ALE of total destruction of the building; compare the two numbers. Is the insurance policy cost-effective? (Hint: in the insurance contract, Megahard bets the insurance company that they will have to pay out $8,000,000 and the insurer bets that they will not pay anything).
16. Why is it so difficult to apply the quantitative risk model to BCP?
17. How does the Generalized Cost Consequence model support BCP?