Business Continuity/Disaster Recovery

Sean Gunasekera

IMS 5002

Week 1 – Security Governance

Week 2 – Managing Security in the organisation

Week 3 – Risk Management

Week 4 – IS security

Week 5 – IS Security

Week 6 – The impact of e-commerce on the organisation

Week 7 – Security over the internet

Week 8 – Security as a critical business function

Week 9 – Risk Management Part 4

Week 10 – Business continuity plans

Week 11 – Security standards, Privacy and law

Week 12 – Current issues and future trends

Week 13 – Revision and exam preparation

Course Outline and Structure

The Problem

The Problem – The Coverage

Gartner Group, October 2001

Source: IDC, July 2004

Recent survey of the Top 5 issues that most concern IT decision makers, 'Disaster Recovery and Business Continuity Planning' came in at number 4.

Business Continuity in the Press

A survey of 430 organisations revealed that of the 138 respondents who could put a figure on losses, 38% said application downtime costs them between £55,000 and £550,000 an hour, with 4% saying it was even more expensive than that.

Computer Weekly; April 16th 2004

According to Gartner Inc, 70% of companies that suffer a major IT disaster without a valid recovery plan, fail within the next year. Of those that do survive, only 10% make a full recovery.

"94 percent of businesses that experience a disaster are out of business within 2 years."

Disaster Recovery Journal

"43 percent of businesses experiencing a disaster never reopen, and 29 percent of those that do reopen close within two years" (U.S. Department of Labor)

Every five years, 20% of companies will suffer a major disruption through fire, flood or storm, power failures, terrorism, or hardware/software failures. Of those companies which do not have a Business Continuity Plan, 80% fail within 13 months of such an incident. Those who successfully restore their business have seen the company value rise.

Source: Business Continuity Institute

Are you worried…!? You should be…

The Answer….

Key Definitions

- **Disaster**: An unplanned outage of sufficient duration to cause unacceptable loss to an organisation

- **Business Continuity Planning**: The process that utilises prevention and crisis management as well as alternate resources and procedures to sustain minimum required business functionality during a crisis. In many cases, prior to IT recovery
Business Continuity has historically been viewed as an Information Technology effort, with minimal input or none at all from Business Process owners. Recent events have proven this to be a defective planning model.

Minimizing Business Continuity risks requires thorough planning! Ensure you have gathered all the business requirements before continuing!

**High Availability (HA)**
Ability to automatically switch to alternate resources when a portion of the system is not or cannot remain functional.

**Business Continuity (BC)**
The process which utilizes prevention and crisis management as well as alternate resources and procedures to sustain minimum required business functionality during a crisis. In many cases, prior to IT recovery.

**Disaster Recovery (DR)**
Provides the technical ability to maintain critical services in the event of any unplanned incident that threatens these services or the technical infrastructure required to maintain them.

Business Continuity includes:

- Security goals
- Risks
- Levels of authority
- How to address security breaches
- Protect people and information
- Set the rules for expected behavior by users, system administrators, management, and security personnel
- Authorise security personnel to monitor, probe, and investigate
- Define and authorise the consequences of violation
- And more…

Business Continuity – Is MORE than protecting computers!

Business Continuity Management involves….

- Assessing and then reducing the risk as far as possible,
- Planning for the resumption of key business processes should a risk materialise and a business disruption actually occur, and
- Testing those plans on a regular basis.

It is not only about IT systems but includes other physical assets such as people, office space and critical documents.

Business continuity management is known by many names including:

- Business continuity planning
- Business strategy planning
- Business continuity management
- Business disruption planning
- Crisis management
- Contingency planning

Business disruption incidents include:

- Environmental disaster: Fire, flood, earthquake etc.
- Acts of terrorism
- Loss of Utilities & Services
- Systems or Equipment Failure
- Information Security Breach
- Malicious Damage
- Civil protest/unrest
- Disruptions in 3rd Parties and Business Partners.

Challenges and Observations

- In BIA it is difficult to break through parochial and departmental view on what is critical and most important.
- In disaster scenarios, changing mindset from ‘normal operations’ to ‘recovery and contingency’.
- Requirements (RTO and RPO) must be balanced by business impact (cost of non-availability) and cost of solution. This makes the method an iterative process balancing requirements, cost, schedule etc.
- Prerequisite for good BIA basis is decent venn diagram, business process, system architecture and business to system mapping. If this does not already exist it can be a huge undertaking. Our amount of reuse in this area is not good.

Sounds Good….?
So How Do I Build It?
Business Continuity Planning – The process

Overview

1. Define objectives and assumptions
2. Gather facts and analyse requirements
3. Draft assumptions on business critical IT services/ systems
4. Design the strategies
5. Implement the plan
6. Test the plan
7. Review/Update/Maintain the plan

Key Questions:
- What are the key business critical processes?
- What are my key physical assets?
- How long can my business survive without these services?
- How will the business impacts be?
- What people, processes, infrastructure do I need in place to recover?
- What are my key physical assets?
- What is the scope of the business continuity project?
- What are any current assumptions the organisation may have?
- What are the key threats the organisation faces?
- What can the organisation do to protect against identified risks (the wished for status)?
- What are the key business critical processes?
- What is the scope of the business continuity project?
- What are any current assumptions the organisation may have?
- What are the organisational impacts?
- What are the business critical processes?
- What are the potential impacts of an incident?
- What is the risk probability?
- What are the key business critical processes?
- What is the scope of the business continuity project?
- What are any current assumptions the organisation may have?
- What can the organisation do to protect the business against identified risks (the wished for status)?
- What are the key business critical processes?
- What is the scope of the business continuity project?
- What are any current assumptions the organisation may have?
- What can the organisation do to protect the business against identified risks (the wished for status)?
- What is the risk probability?
Business Impact Assessment

Identify what processes are important to the business

Business Continuity – The Process
Define Objectives and Assumptions

- Define objectives and assumptions
- Gather facts and analyse requirements
- Develop failure scenarios – recovery scripts
- Identify recovery options
- Undertake cost/benefit analysis

Design the strategies

- Create the plan
- Implement the plan
- Test the plan
- Review, sustain, maintain the plan

Prevention Strategy Mitigation Strategy

- Early warning detection
- Contingency agreements
- Detailed business continuity plans
- Work around solutions
- Minimized data and information

Business Continuity – The Process
Developing Failure Scenarios – Recovery Scripts

- A recovery script is a document that provides step-by-step instructions about:
  - The process required to recover the system
  - Who will complete each step
  - The expected time for long steps
  - Dependencies between steps
  - Why

- A script is necessary because it helps you:
  - Develop and use a proven series of steps to restore system
  - Prevent missing steps
  - Missing a critical step may require restarting the recovery process from the beginning, which delays the recovery.

Recovery Strategy

- Identified and tested business recovery plans
- Comprehensive recovery packages
- Prearranged assets, personnel, external support (and continued relationship

Recovery Process

To reduce recovery time, define a process by:

- Completing as many tasks as possible in parallel
- Adding invenables for each task

During a potential disaster, anticipate a recovery by:

- Collecting facts
- Recalling the latest offsite tapes
- Calling required personnel
- Preparing local operations (sales, finance, and shipping) for alternate procedures for key business transactions and processes.

Recovery process continued

- Minimize the effect of the disaster by:
  - Stopping all additional transactions into the system
  - Waiting too long could worsen the problem
  - Collecting transaction records that have to be manually re-entered
- Begin the planning process by:
  - Analyzing the problem
  - Filling the disaster to your predefined scenario plans
  - Modifying the plans as needed
- Define when to initiate a disaster recovery procedure:
  - What are the criteria to declare a disaster, and have they been met?
  - Who will make the final decision to declare a disaster?
### Recovery process continued

- 5. Declare the disaster.
- 6. Perform the system recovery. 
  - Keep users, who will use a criteria checklist to determine that the system has been satisfactorily recovered should perform the testing.
- 7. Catch up with transactions that may have been handled by alternate processes during the disaster.
  - Once completed, this step should require an additional sign-off.
- 8. Test and sign off on the recovered system. 
  - Key users, who will use a criteria checklist to determine that the system has been satisfactorily recovered should perform the testing.
- 9. Notify the users that the system is ready for normal operations.
- 10. Conduct a postmortem debriefing session. 
  - Use the results from this session to improve your disaster recovery planning.

### Business Continuity – The Process

#### Define Objectives and Assumptions

1. Define objectives and assumptions
2. Gather facts and analyze requirements
   - A. Risk Assessment
   - B. Business Impact Assessment
3. Design the strategies
4. Create the plan
5. Test the plan
6. Implement the plan
7. Test the plan
8. Maintain the plan

#### Test the plan

- Essential!
- A plan is useless without testing!
- Different types of tests needed for different scenarios
- Must always have executive management support

#### Maintain the plan

- Essential!
- A plan is useless without testing!
- Different types of tests needed for different scenarios
- Must always have executive management support

### Security: The benefits

#### Costs vs Benefits

**Benefits**
- Reduced Security Incidents
- Increased Opportunities
- Improved Productivity
- Cost Savings

**Costs**
- Risk Analysis & Business Impact Assessment
  - Very time consuming. It is very subjective and often best practice is not ‘perfect’
- Contingency Costs
  - Contingency costs must be weighed against the downtime costs. Very subjective!
- Professional Services
  - Most large organisations cannot do this alone.
  - Auditors/consultants - $$$$

**... vs...**

Is it worth it? I believe so…
Where else can I get information?
- Free publications:
  - Disaster Recovery Journal
  - Contingency Planning & Management
- Web Sites:
  - www.drj.com
  - www.contingencyplanning.com
  - www.disaster-resource.com
  - www.disaster-resource.com
  - www.isaca.org
  - www.fema.gov
  - www.mcsafe.com
- Online Data security email
  - CSOonline.com.au

References:
- Slide 27 + 28 – Taken from:
- Slide 21 – Taken from: