Overview

- BCP: Definition
- BCP: Need for (Why?)
- BCP: When
- BCP: Who
- BCP: Components
- BCP: Document
- BCP: Guidelines
- BCP: Examples (9/11, SIAC, POSA)
- BCP: HW
BCP Definition

- SANS Institute
  - Business Continuity refers to the activities required to keep your organization running during a period of displacement or interruption of normal operation.

- Business Continuity Institute
  - 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.

- Stan
  - The planning that needs to be done before something bad, unpreventable and most likely irreversible happens to your business.
  - This way, if it really does happen, you won’t be caught off guard and you’ll know how to keep your business open and continue to provide your services.
BCP: Why?

- Disasters will happen
  - We can pray that they don’t
  - We can pretend that nothing bad will happen
  - We can ignore them completely
- Bottom line is that there will always be some risks that will not be preventable but which can have devastating effects on a company’s ability to administer and provide it’s services.
  - Doesn’t matter if you need them 24/7 or 1/7
  - If your services are mission critical, you need to plan for the worst.
  - Don’t just plan on how you’ll restore service.
  - Plan on how you’ll continue providing it in case of a disaster.
- Minimize
  - Money Loss
  - Customers Loss
  - Time Down
  - Confusion
  - Loss of Business Operations
BCP: When do we need it?

- We need to invoke a Business Continuity Plan when there is a disruption to our business such as disaster.
- We need to make the BCP way before a disaster happens, usually in parallel with Risk Mitigation.
- The Business Continuity Plan should cover the occurrence of following events:
  - Equipment failure (such as disk crash).
  - Disruption of power supply or telecommunication.
  - Application failure or corruption of database.
  - Human error, sabotage or strike.
  - Malicious Software (Viruses, Worms, Trojan horses) attack.
  - Hacking or other Internet attacks.
  - Social unrest or terrorist attacks.
  - Fire
  - Natural disasters (Flood, Earthquake, Hurricanes)
BCP: Who is responsible

- Everybody is responsible for contributing.
- Everybody is responsible for executing.
- Everybody is responsible for knowing.
- Designate a Business Continuity Coordinator
  - Responsible for coordinating efforts to maintain the plan.
  - Responsible for coordinating efforts to update the plan.
BCP: Components

- Contingency Planning/Disaster Recovery
  1. destructive measures
  2. response procedures and continuity of operations
  3. determination of backup requirements
  4. development of plans for recovery actions after a disruptive event
  5. development of procedures for off-site processing
  6. guidelines for determining critical and essential workload
  7. team member responsibilities in response to an emergency situation
  8. emergency destructive procedures
Developing a BCP

- **Consider**
  - The use of planning aids, plan development and maintenance tools
  - Inclusion of job descriptions for those involved in delivering the plan
  - What action plans and checklists should be provided
  - What information databases and other supporting documentation are required
  - Define Disaster
  - Define steps of escalation in declaring a disaster

- **Include**
  - The recovery team description, responsibilities and organization
  - Support staff required including recovery and group coordinators
  - The location and equipping of the Emergency (Crisis) Operations Centre
  - A procedure should also be established to shift from the emergency response plan to the business continuity plan.
Developing BCP

- Allocate tasks and responsibilities
  - Differentiate between recovery and departmental teams
  - Identify task to be undertaken
  - The teams required to perform required tasks and their responsibilities
  - Identify and list key contacts, suppliers and resources.
  - The communications required to inform stakeholders and media.
- Identify Mission critical processes and functions
- Identify resources
- Identify how to restore these resources
  - The use, location and protection of critical information and documentation.
  - The requirements for workspace covering critical functions
  - The telecommunications requirements of the operations
  - The essential personnel requirements to deliver the agreed level of service
Developing BCP

The plan should integrate into other key plans:

- Crisis Communications and Public Relations
- Safety and Emergency plans
- IT and Communications Recovery
- Security
- Departmental operating plans
- Supply Chain logistics
- Operational Risk Management
Writing BCP: Include these

- General Introduction and Overview
  - Objectives
  - Responsibilities
  - Exercising
  - Maintenance

- Plan Invocation
  - Disaster declaration
  - Damage assessment
  - Continuity Actions and Procedures
  - Team organization and responsibilities
  - Emergency (Crisis) Operations Centre

- Communications
  - Who should be informed
  - Contacts
  - Key messages

- Suppliers
  - List of recovery suppliers
  - Details of contract provision
Response Procedures and Continuity

- Reporting procedures covering internal and the external communications to the public agencies, media, suppliers and customers.
- Pre-incident preparation based upon the types of incident and to include the management authorities, roles and responsibilities.
- What are the immediate actions are to be taken
- Response procedures
  - Protection of personnel
  - Containment of the incident
  - Assessment of the effect
  - Decisions on the optimum actions to be taken.
  - Crisis Communications with all stakeholders including the media.
  - Taking account of the powers of the public authorities.
- Emergency Operations Center Must establish effective management of any incident (consider these)
  - Location of the operations centre, (taking account of possible cordons created by the public emergency services)
  - Design and equipping the centre
  - Command and decision authority roles during an incident
  - Communications requirements
  - Logging and documentation methods.
- Establish a procedure for command and control
  - Opening the Emergency operations centre and its security arrangements
  - Scheduling of the teams to man the centre and the supply of food and welfare facilities for the teams
  - The management and operations of the centre
  - Closing down of the centre when the crisis has ended.
Development of Plans for Recovery

Actions

- Protecting the organization
  - Board Level decisions must be made
  - Possible choices
    - Do nothing – in some instances the board may consider the risk commercially acceptable
    - Changing or ending the process – deciding to alter existing procedures must be done bearing in mind the organisation’s key focus
    - Insurance – provides financial recompense / support in the event of loss, but does not provide protection for brand and reputation
    - Loss Mitigation – tangible procedures to eliminate / reduce risk
    - Business Continuity Planning – an approach that seeks to improve organisational resilience to interruption, allowing for the recovery of key business and systems processes within the recovery time frame objective, whilst maintaining the organisation’s critical functions.

- Actions:
  - Identify possible Business Continuity strategies
  - Assess suitability of alternative strategies against the output of the BIA
  - Prepare cost / benefit analysis of various strategies
  - Present recommendations to sponsors for approval
Development of Procedures for Off-site Processing

- **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.

- **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.
Development of Procedures for Off-site Processing
Development of Procedures for Off-site Processing

- 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.
Guidelines for Determining Critical and Essential Workload

- Understand the business
- Establish what is vital for its survival
- BCM/BCP must focus on the mission critical processes
- There are four basic questions to be asked:
  - What is this business about?
  - When are we to achieve our goals?
  - Who is involved, both internally and externally?
  - How are the goals to be achieved?
- Identify Dependencies (Internal/External)
  - Suppliers
  - Customers
  - Shareholders
  - IT systems
  - Manufacturing processes
- Get involvement from dependency representatives
- Understand Influence of External Dependencies
  - government departments
  - Regulators
  - Competitors
  - Trade bodies
  - Pressure groups
Guidelines for Determining Critical and Essential Workload

- **Physical Incident**
  - A need to identify the immediate loss mitigation and salvage requirements
  - Understand the need for and, if necessary, prepare an action plan for site safety, security and stabilization.
  - Identify methods of protecting on site assets, including equipment, premises, data and documentation.
  - A need to establish liaison with the external agencies
Guidelines for Determining Critical and Essential Workload

- **Understanding business Actions:**
  - Identify mission critical processes and functions
  - Identify key internal and external dependencies upon which these rely
  - Identify external influences that may impact upon critical processes and functions

- **BIA [business impact assessment] Actions:**
  - Determine impact on business of loss of mission critical process / functions
  - Ensure involvement of appropriate functions
  - Apply rating, including time dependencies
  - Obtain sponsor’s approval to BIA output

- **Risk Assessment Actions:**
  - Determine the threats to critical processes/functions
  - Examine existing risk strategies/analysis
  - Apply scoring system to risks identified
  - Produce combined BIA and RA ranking to identify key focus for BCM
  - Obtain sponsor’s approval to BIA/RA output
Team Member Responsibilities in Emergency Response

- Coordinator is responsible for coordinating efforts
  - Establish
  - Maintain
  - Modify
  - Audit

- Department President and VPs
  - Liaison with BCP Coordinator and low level staff
  - Understand the business process of the company
  - Keep the Departmental BCP updated

- Low level employees
  - Know the plan
  - Understand own responsibilities and expectations during business
  - Know whom to contact and how
Exercising Plan

- Establish a meeting of key recovery staff
- Prepare a representative and suitably detailed disaster scenario. Include aspects such as date, time, current workload, political and economical conditions, accounting period end, concurrent activities.
- Initiate the exercise as a walk-through or a full system test by summarizing circumstances. Consider whether to vary those published, for example by substituting for a key player.
- Document and evaluate exercise results, amending the Plan where necessary.
Maintenance

- Define Plan maintenance scheme and schedule
- Monitor activities
- Update Plans
- Distribute under formal change control procedures
- Plan Audit
Auditing

- Set audit objectives and scope
- Assess and select the audit method
- Audit the administrative aspects of the BCM process
- Audit the Plan’s structure, contents and actions sections
- Audit the Plan’s documentation control procedures
- Submit to the sponsor
BCP: Examples

- 9/11 – success stories
- 9/11 - failures
- SIAC BCP
- POSA Example
Business Stats

- Nearly 1 in 5 businesses suffer a major disruption every year.
  - BCI
- Most businesses experience 2 hours of downtime per week
- Approximately 30% of computer users spend one week per year reconstructing lost data
- 52.2% of U.S. Companies had business operations interrupted due to computer hardware problems
- 43.1% of U.S. Companies had business operations interrupted due to computer software problems
- 46% of U.S. Companies have had business operations interrupted because of telecommunications failure
Post 9/11

Post 9/11, many businesses are reevaluating their contingency plans

- Pre 9/11 – 65% surveyed businesses had plans in place
- Post 9/11 - >50% considered plans to be inadequate

From IDC “How will the World Trade Center disaster affect the Disaster Recovery market?”
Verizon’s Experience in Business Continuity

On September 11, 2001, Verizon lost the 140 West Street building which included a major switching center for the area.
Verizon’s Experience in Business Continuity

Entrance to the West Street building that was heavily damaged by the collapse of the WTC. West Street housed a major Central Office and Switching Center as well as facilities for operations and support staff.

View of damaged New York City E911 switching system.

This switching system was replaced by a new switching system in an alternate location in Southern Manhattan.
Verizon’s Experience in Business Continuity

Assessing the WTC Damage

- Access lines out of service (voice) 200 K
- PBX / Centrex lines out of service 150 K
- Data circuits out of service ~4 Million
- Cell sites out of service 10
- Major Computer Systems 3
- Number of customers affected:
  - Business approx. 14 k
  - Residential approx. 20 k

Landline and Wireless network call completions were at least 2 times higher than normal levels on Sept. 11
Verizon Expertise in BRCS

Verizon’s Response to our customers:

- **Network Capacity Added:**
  - 18 New SONET Rings Built
  - 21 Temporary Cellular Towers Erected
- **Computer Systems recovered within 24 hrs at alternate sites.**
- **3,000 technicians and managers deployed in Southern Manhattan.**
- **4,000,000 Voice and Data Circuits constructed, repaired, or re-routed within first week**
- **Aggressive Deployment of Centrex, ISDN, DSL, Video and Audio conferencing**

Verizon recovered and rerouted the Securities Industry Data Network to allow the NYSE to open on 9/17.
Verizon’s Commitment to Business Continuity

Verizon Network Engineering and IS Operations have a legacy of providing extremely high availability.

Depth and breadth of services
- 6300 Central Offices and Raised Floor space
- 1.5M square miles of service area
- 50 Mainframes, 5000+ Unix systems and 100K PC’s with Mission Critical Recovery in 24 hours.
- ISO 9002 Certifications for IS Operations and Business Continuity
- Presence in 41 international locations with operations in 21

Strategic Business arrangements
- Leverage Verizon’s own experience in contingency planning and restoration
- Alliance agreements with major I/S Hardware, Software and Consulting firms.

“Our reputation for service and reliability is part of our heritage, and an integral part of our customer commitment”
More 9/11

- Small Stockbrokerage Company with no BCP
  - Was Relocating to NJ facility from WTC, just days prior to 9/11
  - Had a complete mirror of all hardware and software at the NJ site.
  - When disaster struck and old site was destroyed, the company wasn’t affected because they were ready to migrate all along (were already migrated)
  - Really Lucky in this regard
    - If they had a BCP, it would have told them to have a mirrored back – up site, which they ended up having inadvertently.
    - If they didn’t have to move, they would have most likely been out of business.
Examples: SIAC

- BCP training
- BCP practice
- Mirrored Dual Site Processing
- Special Day Off
- BCP Emergency Contact Card
- BCP Updating Contact Info
Examples: POSA

- POSA system becomes unavailable
  - Employee Intervention
  - Software/Hardware Malfunction
    - Have several POSA machines available
    - Have warranty/insurance
  - Link Malfunction
    - Have several links to the Server

- Credit Card Authentication Service becomes unavailable
  - Main transaction processing server outside the control of the store goes out of service.
    - Provide ATMs around the store (customers can use ATM to get cash to pay.)
    - Provide Own Store Credit Card, so as not to rely on outside authentication services.
BCP: HW

- For the GTS Server Example create a part of the BCP
  - Define what constitutes a disaster
  - Define the minimal level of service expected during a disaster
  - Define what actions could be taken to provide at least the minimal level of service
  - Define the proper communication channel procedures in case of disaster
    - Who should be contacted and how
    - How is this information disseminated
References

  - Pages 230-244
- “Verizon Business Recovery And Continuity Services”
Further Resources

- “General Business Continuity Terms” Business Continuity Institute Glossary.
  - URL: http://www.dr.org/model.htm (21 Aug. 2001)