MIS 131: Information Systems Administration

Part V: IT Security

Section B: Business Continuity Planning

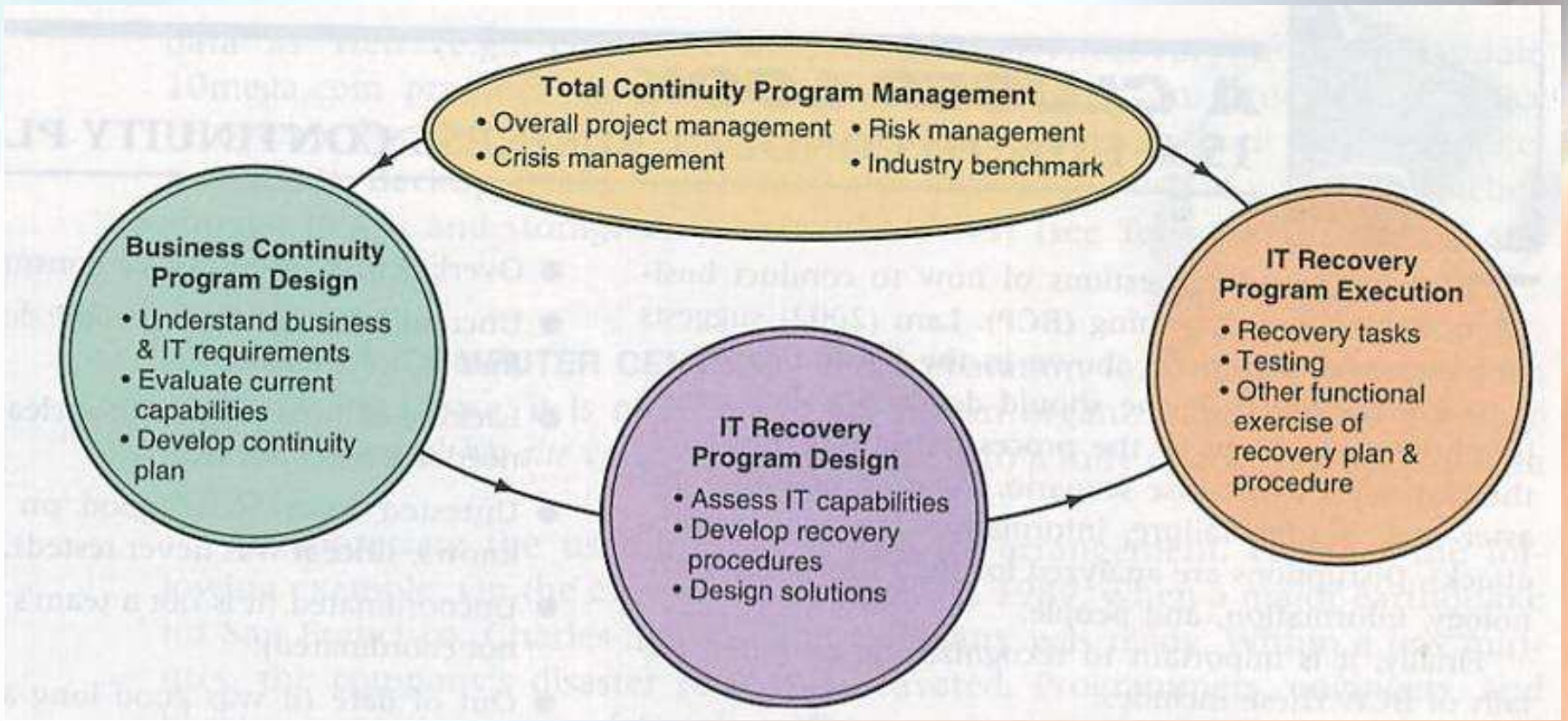
The Need to Be Prepared

- Disasters occur without warning and the best defense is preparedness
- Advance crisis planning can help minimize losses
- An important element in any security system is the *business continuity plan*

Business Continuity Plan

- Also known as *business process contingency plan*
- Purpose is to keep critical business functions running with minimal or no interruptions after a disaster occurs
- Also outlines the process by which businesses would recover from a major disaster

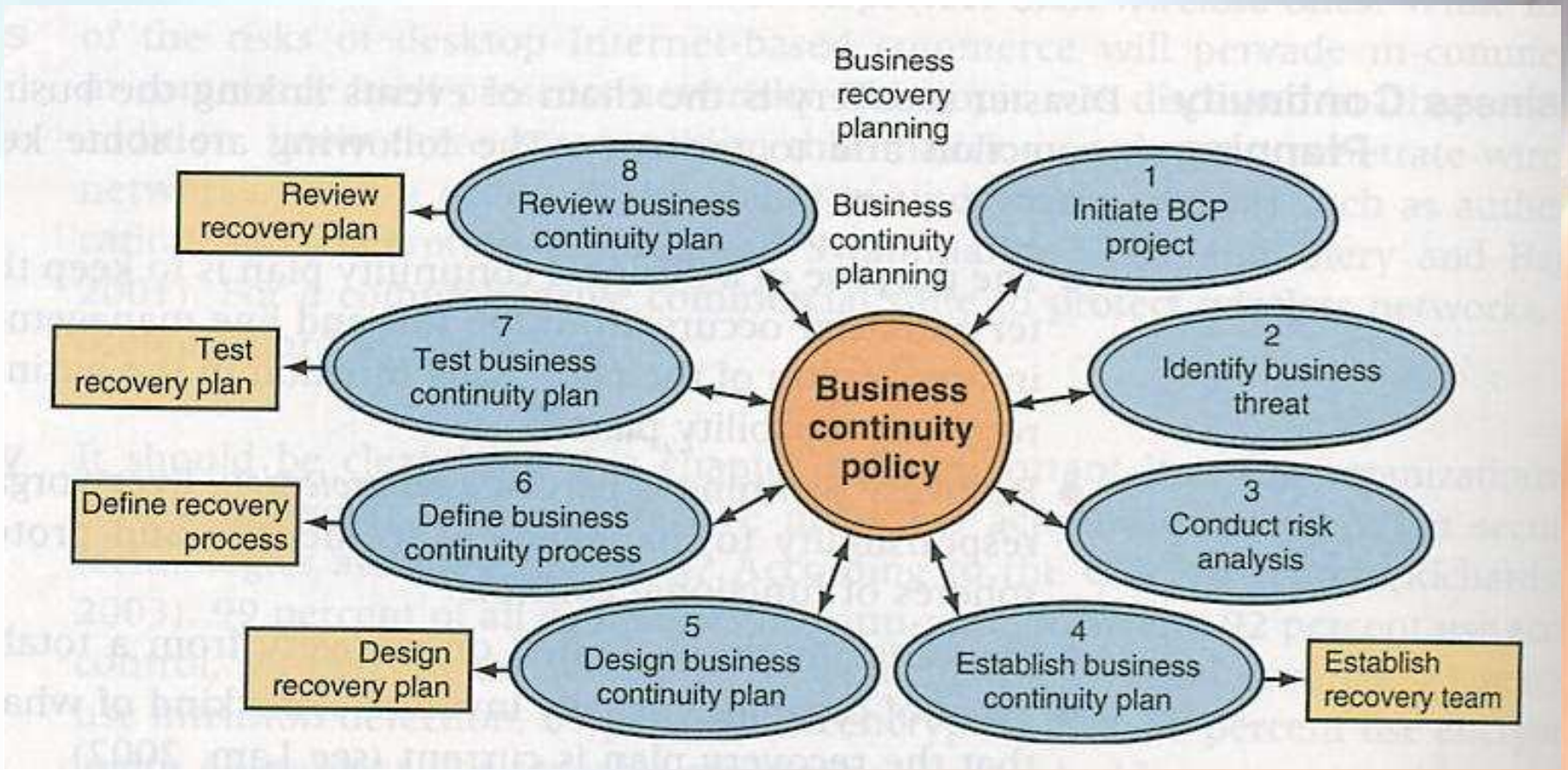
The Comprehensiveness of a BCP



Disaster Recovery Plan

- Sometimes suggested to be synonymous with BCP, but the two are actually different
- In the IT context, a DRP documents actions to be taken to restore computer processing, applications, telecommunications, and data after a disruption to minimize impact on business
- Considered part of BCP

Steps in BC Planning



BC Planning: Key Thoughts

- Ensures IS is able to recover efficiently and in the least amount of time after a disaster
- Part of asset protection
- Should focus first on recovery from total loss of all capabilities
- Both IS and management should be involved in preparation of plan
- BCP must be tested periodically
- An outdated plan is worse than having no plan at all

BC Planning: Key Thoughts

- BCP should be well-documented and kept in a safe but accessible place
- The plan must be audited regularly
- The plan should be written so that it is effective in case of disaster and not just to satisfy auditors
- All critical applications must be identified and recovery procedures addressed
- Accompanied by management and end-users responsibilities

Management Responsibilities

- Determines scope of BCP
- Determines maximum amount of time for an application to be recovered
- Makes business decisions on recovery alternatives
- Accepts risks for possible exposures
- Accepts responsibility for the continuity of business until IS recovers

User Responsibilities

- Provides input on selection of most critical application systems
- Provides input on maximum amount of time allowable for recovery
- Provides input to management on impact to business of application systems loss, time constraints for recovery, and possible data processing

Backup and Recovery

- Backup: one of the most logical ways to deal with data loss
- Included in BCP
- Backup arrangements
  - Backup of data files
  - Backup of data center

Backup of Data Files

- Backup critical data regularly
- Store backup media both in local (onsite) and remote sites (offsite)
- Practice recovery procedures regularly

Types of Data File Backup

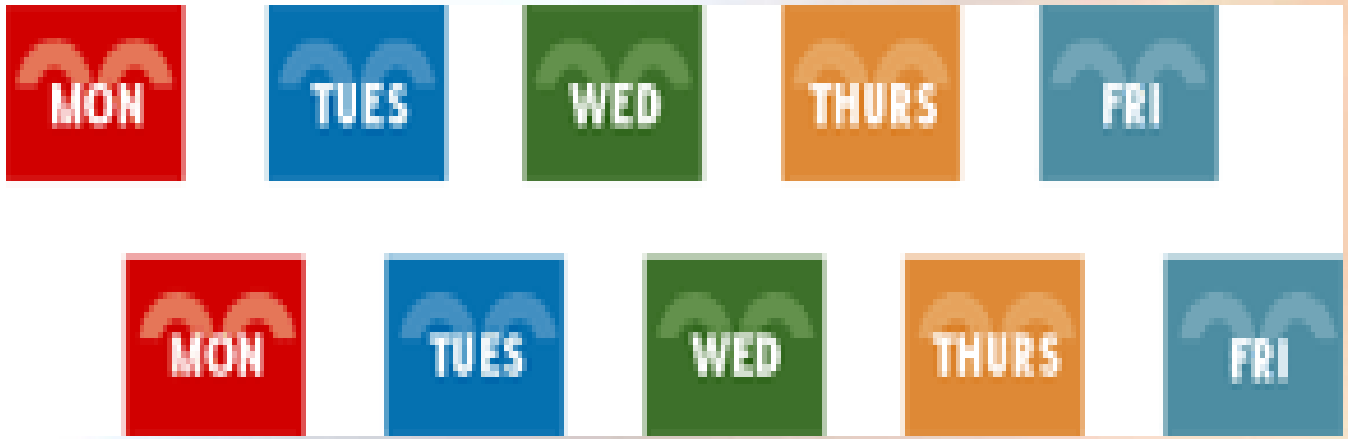
- Full
  - All selected files are backed-up
- Differential
  - New and changed files since last full, regardless whether file changed during last backup or not
- Incremental
  - New and changed files since last backup

Data File Backup Schemes

- No media rotation
  - Only one tape/medium is re-used depending on backup frequency
  - Does not archive history of data
- With media rotation
  - Reuses several media based on pre-determined scheme
  - Popular rotation schemes include
    - Round robin
    - GFS
    - Tower of Hanoi

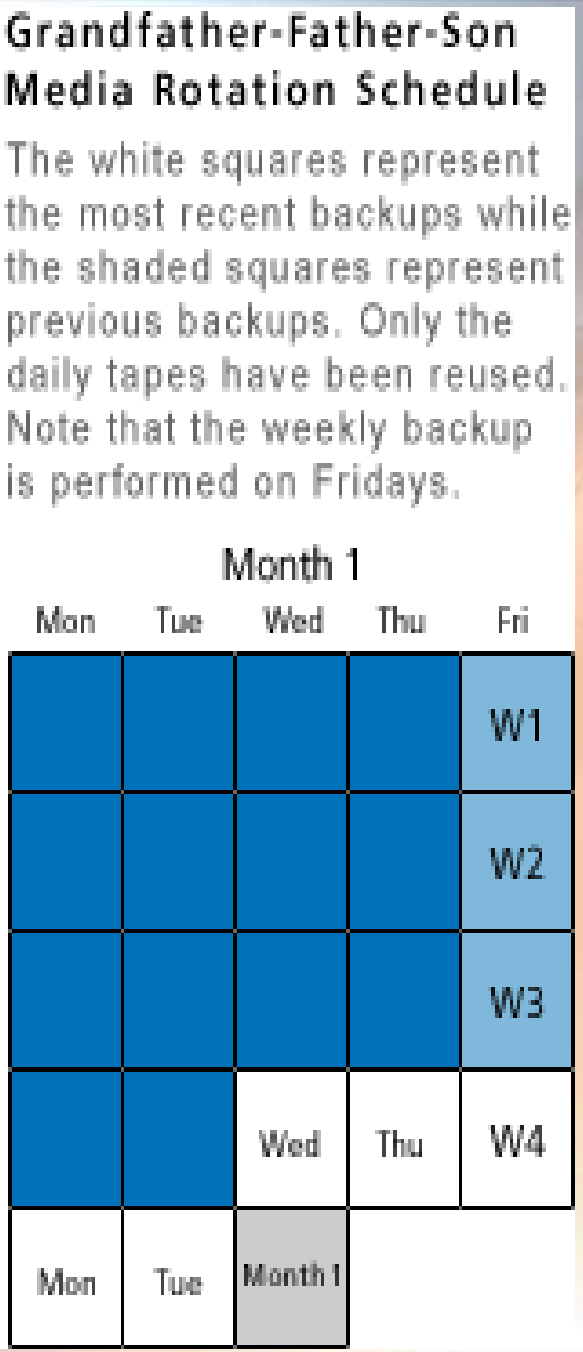
Round Robin

- Uses five tapes (one tape per day of the workweek)
- Does not lose more than a day's worth of data

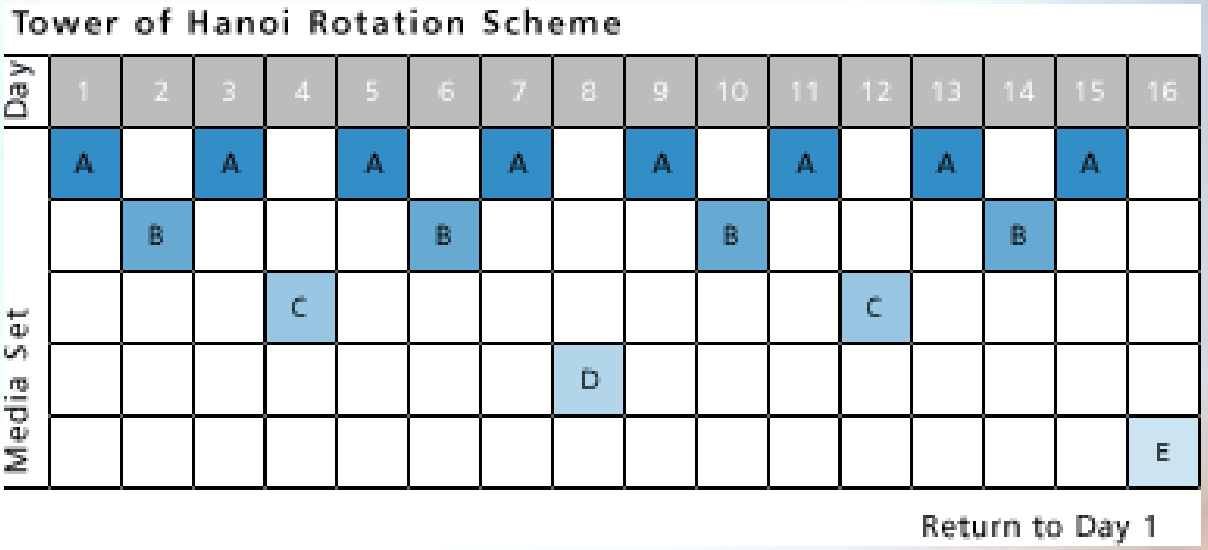


Grandfather, Father, Son (GFS)

- Most common scheme
- Daily – weekly – monthly
- Disadvantage: needs a large number of tapes



Tower of Hanoi



- Based on math puzzle
- Uses full backups
- The more often a media set is used, the more recent the archived data
- Doubles backup history with every additional tape
- Best practice: 8 if daily, 5 if weekly
- Example: 5 dailies
  - –ABACABADABACABA…
- Disadvantage: long backup window

Backup of Data Centers

- Provides location from which recovery can take place
- This location is known as *backup site*
- Where the data center will be recreated and will operate from, for the length of the disaster
- Useless without a definitive BCP

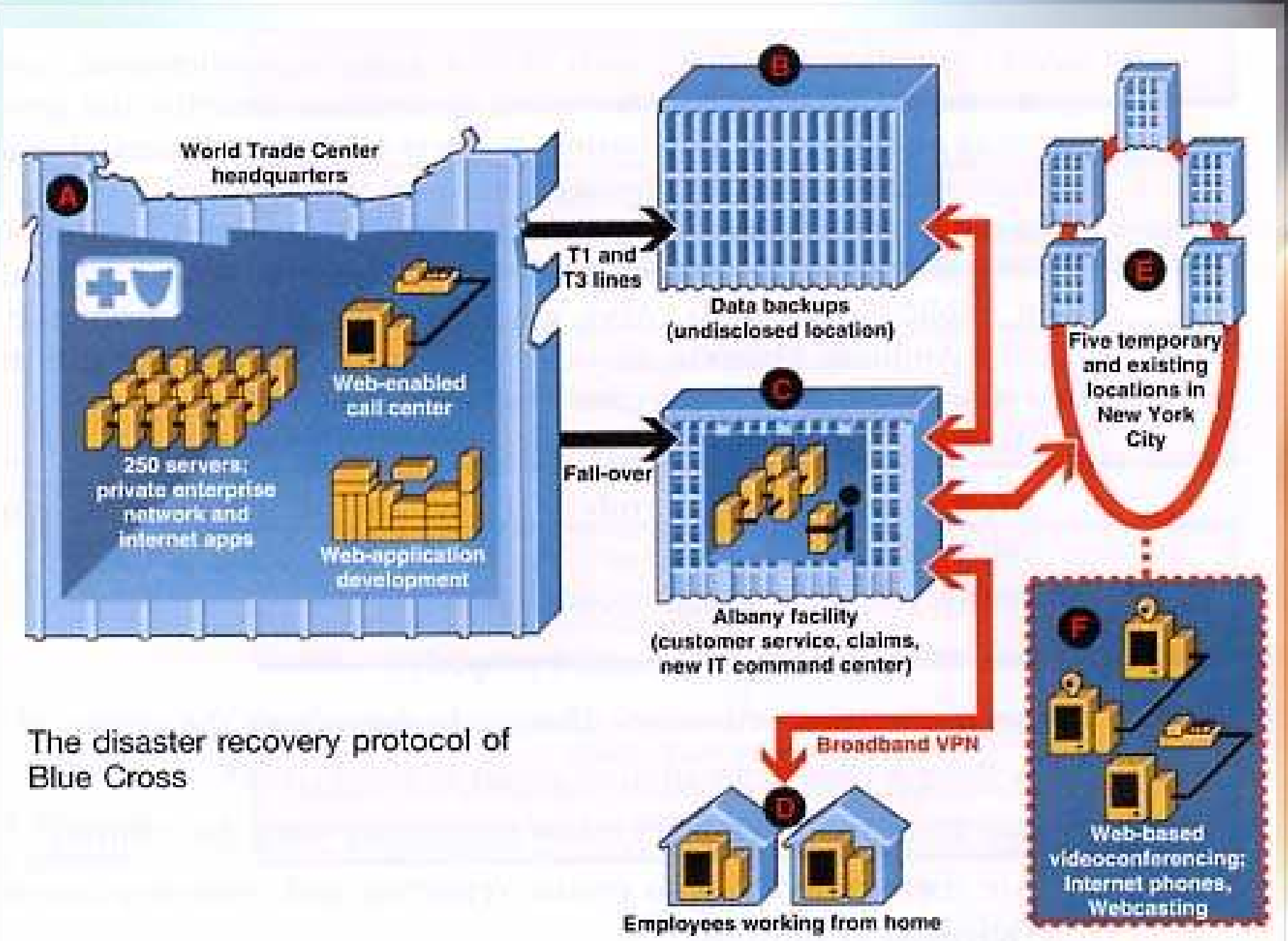
Configuration of Backup Site

- Hot site
  - Fully-configured data center
  - Most expensive
- Warm site
  - With hardware representing reasonable facsimile of what is in current data center
- Cold site
  - Empty space with special flooring, ventilation, and wiring
  - May have substantial delay in switchover

Sources of Backup Site

- Mutual agreement with another company
  - Reciprocated relationship that allows sharing of data center facilities in case of a disaster
- Shared disaster recovery center
  - An arrangement where two or more companies contribute equitably to build a backup data center for recovery purposes
- A second data center
  - Other locations owned and operated by the organization
- Third-party data center
  - Company offering data center space and services

BCP in Action: Blue Cross



The disaster recovery protocol of Blue Cross