CSE 465
Information Assurance

Contingency and Disaster Recovery Planning

Professor Stephen S. Yau

Definitions

- Contingency planning
  - ***Multifaceted approaches*** to ensure ***critical system and network assets to remain functionally reliable***
- Disaster recovery planning
  - ***Seps and procedures*** the personnel in key departments must follow in order to ***recover critical information systems in case of a disaster*** that causes loss of access to systems.

Why We Need Such Planning?

- No 100% secure systems.
- What can we do?
  - Plan for the worst if bad things happen
    - How to restore service?
    - How to continue to provide service in case of any
      incident, including disaster?

When We Need Planning?

- Contingency and disaster recovery planning should be completed for invocation whenever a disruption to the system occurs ***[when?]***
- Possible causes for a disruption include :
  - Equipment failure
  - Power outage
  - Telecommunication network shutdown
  - Software corruption
  - Malicious software attacks
  - Hacking or other Internet attacks
  - Human error
  - Sabotage
  - Strike
  - Terrorist attacks
  - Natural disasters

Plan Components

- Measures of disruptive events
- Response procedures and continuity of operations
- Backup requirements
- Plan for recovery actions after a disruptive event
- Procedures for off-site processing
- Guidelines for determining critical and essential workload
- Individual employees' responsibilities in response to emergency situations
- Emergency destructive procedures

Measures of Disruptive Events

- ***Identify and evaluate possible disruptive events***:
  - Identify most ***critical processes and requirements*** for continuing to operate in the event of an emergency
  - Identify ***resources*** required to support most critical processes
  - ***Define disasters*** and ***analyze possible damage*** to most critical processes and their required resources
  - Define ***steps of escalation*** in declaring a disaster

Response Procedures and Continuity of Operations

- Reporting procedures
  - ***Internal:*** notify IA personnel, management and related departments
  - ***External:*** notify public agencies, media, suppliers and customers
- Determine ***immediate actions*** to be taken after a disaster happens
  - Protection of personnel
  - Containment of the incident
  - Assessment of the effect
  - Decisions on the optimum actions to be taken
  - Taking account of the power of public authorities

Backup Requirements

- Critical data and system files must have backups stored ***off-site***. Backups are used to
  - ***Restore data*** when normal data storage is unavailable
  - Provide ***online access*** when the main system is down
- Not all data needs to be ***online or available at all times***
  - Backup takes time and need additional storage space
  - Require extra effort to keep backup ***consistent with normal data storage***
  - Backup should consider ***data-production rates, data-loss risk*** and ***cost effectiveness***

Backup Requirements (cont.)

- Decide ***what and how often*** to backup depends on ***risks:***
  - ***Immediate loss of services***: In case of power failure or application crash, any data that has not been saved will be lost. If the data is critical, users must be aware of this risk and make periodic "saves" themselves
  - ***Media losses***: storage media has physical damage and can no longer be read. Need to decide
    - How often to do a complete backup?
    - Will incremental backups be done between two complete backups?
    - What media will be used for backup?
  - ***Archiving inactive data***: recent active data should be put onto a hard disk for fast access, while old inactive data can be archived to tape, CD or DVD in order to free hard disk space

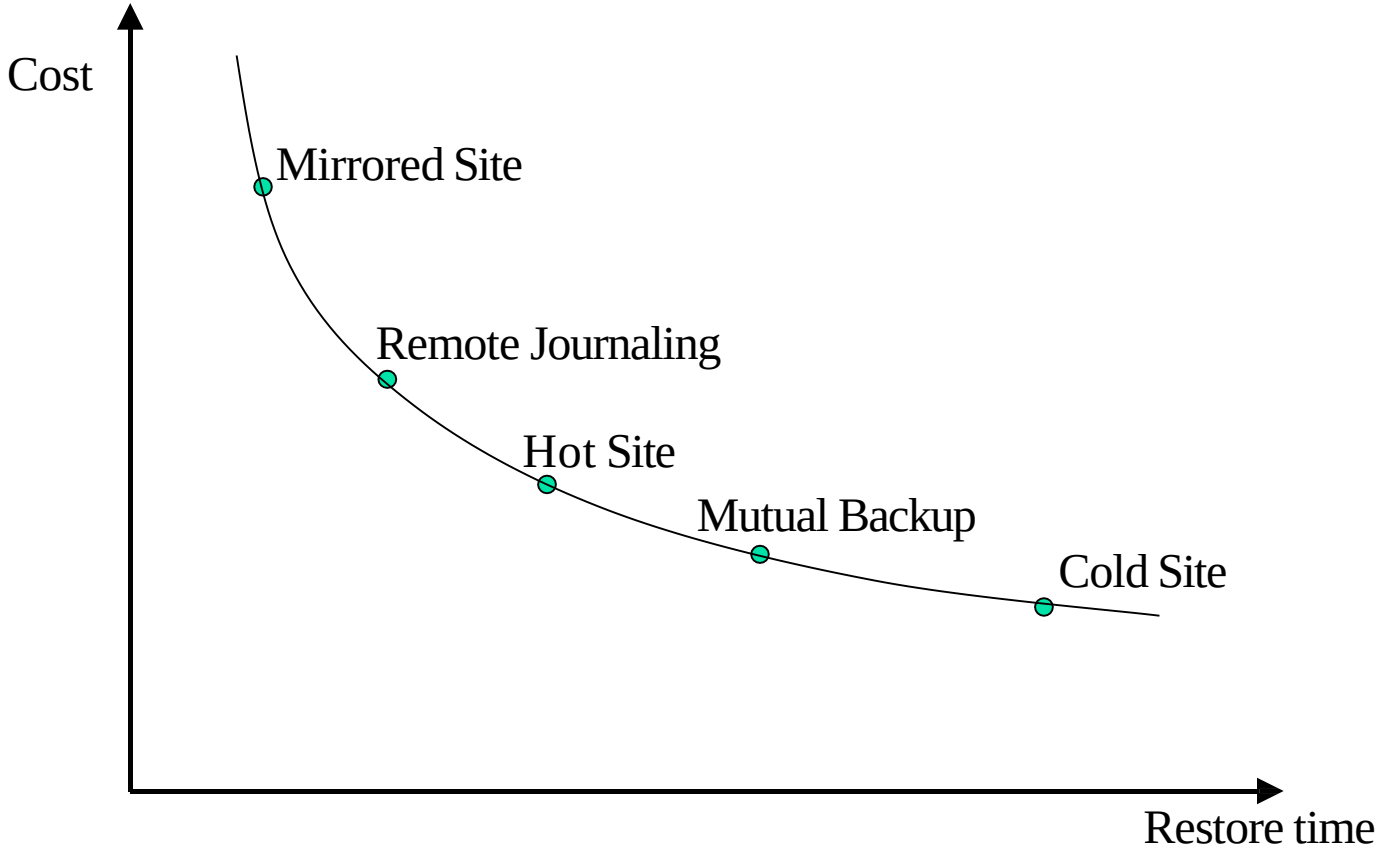
Plan for Recovery Actions

- ***High-level management*** must decide what the organization should do after a disruptive event happens. Possible choices:
  - ***Do nothing:*** loss is tolerable; rarely happens and cost more to correct it.
  - ***Seek for insurance compensation:*** provides financial support in the event of loss, but does not provide protection for the organization's reputation.
  - ***Loss mitigation:*** isolate the damage and try to bring the system back online as soon as possible.
  - ***Bring off-site system online for continuous operation:*** maintain an off-site backup system that will kick in when a disruptive event has made the original system unavailable.
- Identify all possible choices, including cost/benefit analysis and present recommendations to high-level management for approval.

Off-site Processing

- Choices for off-site processing:
  - ***Cold site***: an empty facility located offsite with necessary infrastructure ready for installation of back-up system in the event of a disaster
  - ***Mutual backup***: two organizations with similar system configuration agree to serve as a backup site for 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 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***

Off-site Processing (cont.)



Decision Factors for Off-site Processing

- Availability of facility
- 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 system's ***mission goal***
- Identify ***mission critical processes***
- Identify ***dependencies*** among various departments/personnel within the organization
- Understand ***influence of external factors***
  - Government agencies
  - Competitors
  - Regulators

Individual Responsibilities in Emergency Response

- ***Emergency response planning coordinator***: coordinates the following activities:
  - Establish contingency/disaster recovery plans
  - Maintain/modify the plans
  - Audit the plans
- ***High-level manager*** (department manager, VP, etc.)
  - Understand process and mission goal of the organization
  - Monitor contingency/disaster recovery plans and keep plans updated
- ***All other employees***
  - Know ***contingency/disaster recovery plans***
  - Understand ***own responsibilities and expectations*** during operation
  - Know ***whom to contact*** if something not covered in plan happens

Emergency Destructive Procedures

- Under certain situations, an emergency response may focus on destroying data rather than restoring data
  - Physical protection of system is no longer available
  - Critical assets (product design documents, list of sensitive customers or suppliers, etc.)
- An emergency destructive plan should contain
  - ***Prioritized items*** that may need to be destroyed
  - ***Backup procedure*** for critical data at a secure off-site location
  - Specify ***who has authority*** to invoke destructive plan

Testing Contingency/ Disaster Recovery Plan

- Testing is a necessary and essential step in planning process:
  - A plan may look great on paper, but until it is carried out, no one knows how it will perform
  - Testing not only shows ***the plan is viable***, but also prepares ***personnel involved by practicing their responsibilities and removing possible uncertainty***

Testing Contingency/ Disaster Recovery Plan (cont.)

- Five methods of testing such a plan
  - **Walk-through**: members of key units meet to trace their steps through the plan, looking for omissions and inaccuracies
  - **Simulation**: during a practice session, critical personnel meet to perform dry run of the emergency, mimicking the response to true emergency as closely as possible

Testing Contingency/ Disaster Recovery Plan (cont.)

- **Checklist**: more passive type of testing, members of the key units "check off" the tasks on list for which they are responsible.Report accuracy of the list
- **Parallel testing**: ***backup processing*** occurs in parallel with ***production services that never stop***. ***If testing fails, normal production will not be affected***.
- **Full interruption**: ***production systems are stopped*** as if a disaster had occurred to see how backup services perform

References

- Michael E. Whitman, Herbert J. Mattord , *Principles of Information Security, Thomson* Course Technology, 5th edition, 2014.
- Mark Stamp, *Information Security: Principles and Practice*, 2nd Edition, 2011
- Michael E. Whitman, Herbert J. Mattord , *Principles of Information Security*, Course Technology, 2011
- Mark Stamp, *Information Security: Principles and Practice*, Wiley, May 2011, 606 pages, ISBN-10 0470626399