ACS-2821-001
Information Security in Business

Business Continuity Planning and Disaster Recovery Planning

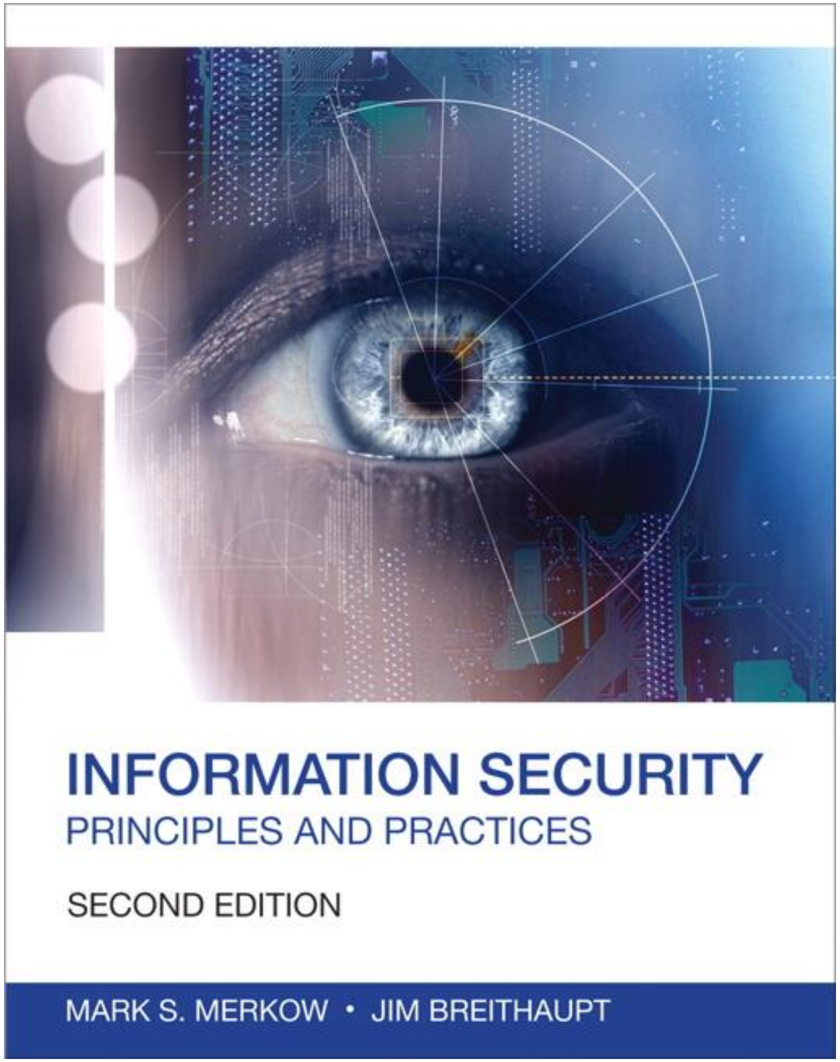
ACS-2821-001 – Slides Used In The Course

A note on the use of these slides:

These slides has been adopted and/or modified from the original for the use in this course. The author of the text have make these slides available to all (faculty, students, readers) and they obviously represent a *lot* of work on their part.

In return for use, please:

- If slides are being used (e.g., in a class) that the source be mentioned (after all, the author like people to use our book!)
- If any slides are being posted on a www site, note that they are adapted from (or perhaps identical to) the author original slides, and note their copyright of this material.



INFORMATION SECURITY

PRINCIPLES AND PRACTICES

SECOND EDITION

MARK S. MERKOW • JIM BREITHAUPT

Objectives

- Distinguish between the business continuity plan (BCP) and the disaster recovery plan (DRP)
- Follow the steps in the BCP
- Explain to business executives why planning is important
- Define the scope of the business continuity plan
- Identify types of disruptive events
- Outline the contents of a business impact analysis (BIA)
- Discuss recovery strategies and the importance of crisis management
- Explain backup and recovery techniques, including agreements for shared sites and alternate sites

Overview of the Business Continuity Plan and Disaster Recovery Plan

- Business continuity planning and disaster recovery planning
  - Share the common goal of keeping a business running in the event of an emergency or interruptions
- Business continuity plan (BCP)
  - Describes the critical processes, procedures, and personnel that must be protected in the event of an emergency
  - Uses the business impact analysis (BIA) to evaluate risks to the organization and to prioritize the systems in use for purposes of recovery
- Disaster recovery plan (DRP)
  - Describes the exact steps and procedures personnel in key departments must follow in a disaster

Why the BCP Is So Important

- 80% of businesses without a recovery plan either closed or never reopened within 18 months
- 70% of companies go out of business after a major data loss
- 80% of companies without a BCP fail within 2 years
- 60% of companies that lose their data shut down within 6 months of a disaster

Source: Continuity Central, http://continuitycentral.com/feature0660.html

Steps for business continuity planning

Business Continuity Planning Steps:

1. Identify the scope and boundaries of the business continuity plan
   - This step typically involves an audit analysis of the organization’s assets and a risk analysis
2. Create the business impact assessment
   - The BIA measures the operating and financial loss to the organization resulting from a disruption to critical business functions
3. Present the BCP to key senior management and obtain organizational and financial commitment
4. Each department needs to understand its role in the plan and support and help maintain it
5. The BCP project team must implement the plan
   - BCP must be updated with changes in the organization

Different business unit may have their own BCP in a large organization, as long as it coincide with organization BCP

Types of Disruptive Events

- Natural events
  - Earthquakes, fires, floods, mudslides, snow, ice, lightning, hurricanes, tornadoes, and so forth
  - Explosions, chemical fires, hazardous waste spills, smoke, and water damage
  - Power outages caused by utility failures, high heat and humidity, solar flares, and so forth
- Manmade events
  - Strikes, work stoppages, and walkouts
  - Sabotage, burglary, and other forms of hostile activity
  - Massive failure of technology including utility and communication failure caused by human intervention or error

Defining the Scope of the Business Continuity Plan

- Identifying critical business processes and requirements for continuing to operate in the event of an emergency
- Assessing risks to the business if critical services are discontinued, referred to as business impact analysis
- Prioritizing those processes and assigning a value to each process
- Determining the cost of continuous operation and the value ascribed to each service
- Establishing the priority of restoring critical services
- Establishing the rules of engagement upon the BCP plan approval

Creating the Business Impact Analysis

- Identifies the risks specific threats pose, quantifies the risks, establishes priorities, and performs a cost/benefit analysis for countering risks
- Seven steps
  - Identify key business processes and functions.
  - Establish requirements for business recovery.
  - Determine resource interdependencies.
  - Determine impact on operations.
  - Develop priorities and classification of business processes and functions.
  - Develop recovery time requirements.
  - Determine financial, operational, and legal impact of disruption.

Recovery Time Requirement Terms

Maximum Tolerable Downtime (MTD)

- The maximum time a business can tolerate the absence or unavailability of a particular business function.
- Different business functions will have different MTDs.
- It correlation between the criticality of a business function and its maximum downtime.
- The higher the criticality, the shorter the maximum tolerable downtime
- It consists of two elements, the systems recovery time and the work recovery time, i.e. MTD = RTO + WRT.

Recovery Time Requirement Terms

Recovery Time Objective (RTO)

- First segment of the maximum tolerable downtime (MTD)
- The time available to recover disrupted systems and resources.

Work Recovery Time (WRT)

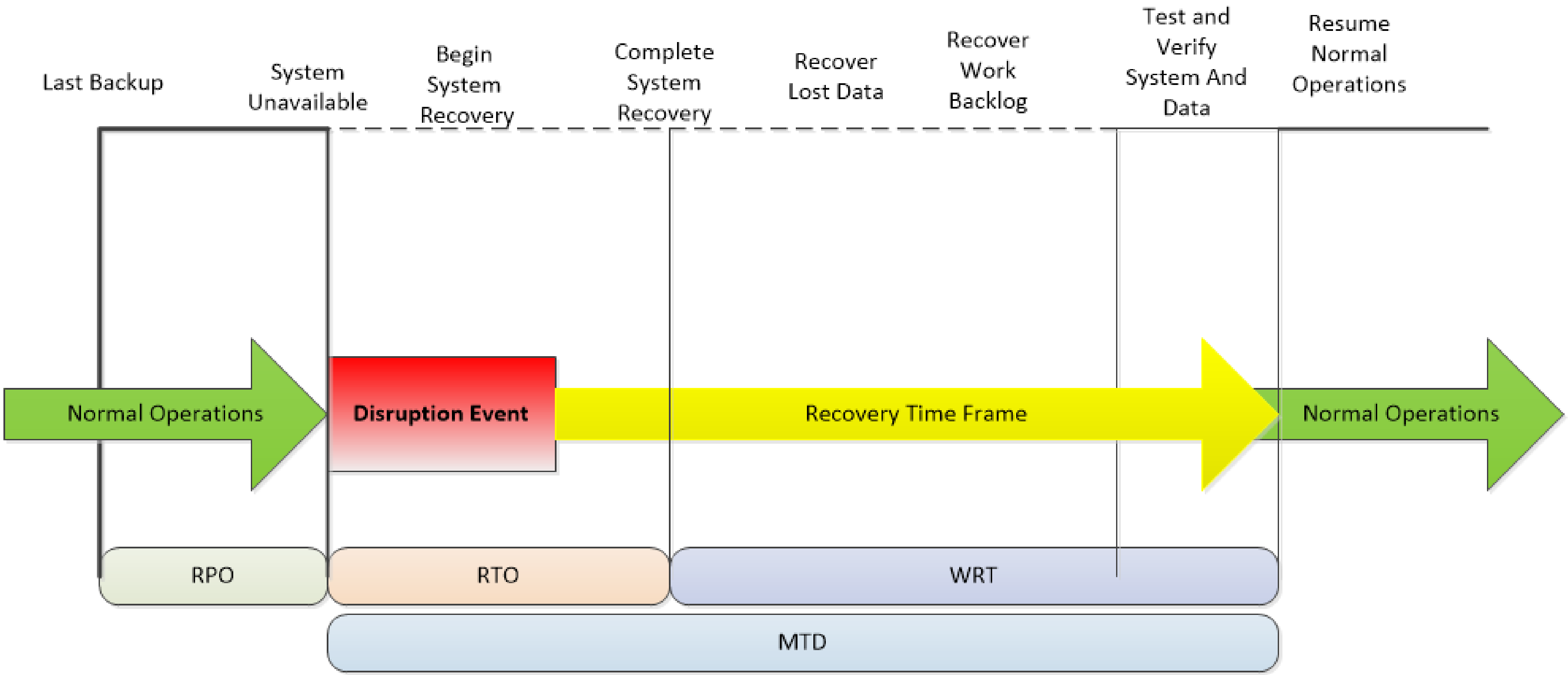
- The second segment that comprises the maximum tolerable downtime (MTD)
- It is the time to get critical business functions back up and running once the systems (hardware, software, and configuration) are restored.
- From an IT perspective once the systems are back up and running, recovery is complete.
- But from a business function perspective, additional steps maybe require before it's back to business.

Recovery Time Requirement Terms

Recovery Point Objective (RPO)

- The amount or extent of data loss that can be tolerated by your critical business systems.
- It is based on current operating procedures and your estimates of what might happen in the event of a business disruption.
- It's important to define your RPO in order to ensure your recovery processes address these timelines.

Disaster Recovery Timeframe



Disaster Recovery Planning

- The goals of the DRP
  - Keeping the *critical systems/computers* running
    - During and post disaster
  - Meeting formal and informal service-level agreements with customers (internal and external) and suppliers
  - Being proactive rather than reactive
    - Example - using mirrored servers for mission critical systems, maintaining hot sites, training disaster recovery personnel

Key Elements in a DRP

- Provide for the safety and well-being of people on the premises at the time of a disaster;
- Continue critical business operations;
- Minimize the duration of a serious disruption to operations and resources (both information processing and other resources);
- Minimize immediate damage and losses;
- Establish management succession and emergency powers;
- Facilitate effective co-ordination of recovery tasks;
- Reduce the complexity of the recovery effort;
- Identify critical lines of business and supporting functions

Identifying Recovery Strategies

- The BCP will identify the **critical business processes** that must be protected through the BIA documents
- The function of the DRP is to identify the **exact strategy** for recovering those processes, specifically IT systems and services that are struck by a disaster

Identifying Recovery Strategies

- Inventory hardware and software.
- Define your tolerance for downtime and data loss.
  - Recovery point objective (RPO) and Recovery time objective (RTO)
- Lay out who is responsible for what – and identify backup personnel.
- Create a communication plan.
- Let employees know where to go in case of emergency – and have a backup worksite.
- Make sure your service-level agreements (SLAs) include disasters/emergencies.
- Include how to handle sensitive information
- Test your plan regularly.

Backup Strategies

- **Full backup only / System imaging**
  - A full backup makes a complete copy of all data of the business system
  - Advantage - minimal time to restore data
  - Disadvantages - takes longer to perform a full backup and requires more storage space
  - Full backups are typically run only periodically
  - Typically use in combination with either incremental or differential backups

Backup Strategies

- **Incremental**
  - An incremental backups take backup from more points in time and organize the data into increments of change between points in time.
  - a full backup is made on specific timeframe i.e. weekly or monthly and incremental backups are made after successive time periods i.e. daily.
  - Restore will from the last full backup taken before the data loss, and then applying in turn each of the incremental backups since then.

Backup Strategies

- **Differential**
  - Backup the data that has changed since the last full backup.
  - Advantage - only a maximum of two data sets are needed to restore the data.
  - Disadvantage - the time to perform the differential backup increases when the last full backup was done, i.e. accumulated changes in data
  - Restoring an entire system would require starting from the most recent full backup and then applying just the last differential backup since the last full backup.

Backup Strategies - Example

Type/Backup number	Full	Incremental	Differential
Backup 1	All data	--	--
Backup 2	All data	Changes from backup 1	Changes from backup 1
Backup 3	All data	Changes from backup 2	Changes from backup 1
Backup 4	All data	Changes from backup 3	Changes from backup 1

Backup Rotation Scheme

Common backup rotation scheme

- **First in, first out**
  - First in, first out (FIFO) backup scheme saves new or modified files onto the "oldest" media in the set
  - Example - Performing a daily backup using a set of 14 media, the backup depth would be 14 days
  - Advantage - retains the longest possible tail of daily backups
  - Disadvantage - can suffers from the possibility of data loss if error is introduced into the data, but identified until several generations of backups and revisions have taken place. Than all the backup files contain the error

Backup Rotation Scheme

Common backup rotation scheme

- **Grandfather-father-son**
  - A common rotation scheme for backup media
  - Has three or more backup cycles, such as daily, weekly and monthly
  - The daily backups are rotated on a daily basis using a FIFO system as above. The weekly backups are similarly rotated on a weekly basis, and the monthly backup on a monthly basis
  - In addition, quarterly, half-yearly, and/or annual backups could also be separately retained

Understanding Shared-Site Agreements

- Also known as Reciprocal Agreement or Consortium Agreement
- Arrangements between companies with similar data processing centers
- Save time and money
- Could be difficult to implement
  - Legal liability
  - Different company cultures
  - Disaster could strike both parties if they are in physical proximity

Using Alternative Sites

- Three main forms
  - Hot site
    - Contain the equipment needed to continue operation, including office space and furniture, telephone jacks and computer equipment
    - May need to restore data to continue business operation
    - Provide an uninterrupted service
    - Very expensive
  - Cold site
    - Provides only facilities with no hardware or software
    - Business will need to provides and installs all equipment i.e. hardware and software to continue operations
    - Cost effective but it takes longer to set up

Using Alternative Sites

- Three main forms
  - Warm
    - Provides the facilities with hardware
    - May require additional hardware setup from business
    - Software and data must be restored
    - Takes more time to setup than a hot site but less time than a cold site
    - Good for business that has a short RTO
    - Also good for non-mission business system

Making Additional Arrangements

- Multiple sites or Redundant sites
  - Processing distributed across multiple or redundant sites
- Service bureaus
  - Provide backup processing services at remote location
  - Quick response, but high cost
- Mobile units
- The cloud
  - Cloud DR or Cloud Disaster Recovery
  - Provide an infrastructure as a service (IaaS) solution that backs up designated system data on a remote offsite cloud server.
  - Also provides updated recovery point objective (RPO) and recovery time objective (RTO) in case of a disaster or system restore.
  - Can be scaled as needed to meet business growth

Testing the Disaster Recovery Plan

- Checklists
  - A more passive type of testing and a first step toward a more comprehensive test
- Walk-throughs
  - Members of the key business units meet to trace their steps through the plan, looking for omissions and inaccuracies
- Simulations
  - Critical personnel meet to perform a “dry run” of the emergency, mimicking the response to a true emergency as closely as possible

Testing the Disaster Recovery Plan

- Parallel testing
  - The backup processing occurs in parallel with production services that never stop
- Full interruption
  - Production systems are stopped as if a disaster had occurred to see how the backup services perform

Importance of Testing the DRP

- Exercise the recovery processes and procedures
- Familiarize staff with the recovery process and documentation
- Verify the effectiveness of the recovery documentation
- Verify the effectiveness of the recovery site
- Establish if the recovery objectives are achievable
- Identify improvements require to the DR strategy, infrastructure, and recovery processes

Summary

- BCP and DRP are formal processes in any business that is concerned about maintaining its operation in the face of a disaster or interruption
- To implement its DRP a company typically uses outside services
- The plan must be thoroughly tested using one or more of the five testing techniques

ACS-2821-001 – Questions?