Protecting Information Assets
- Week 8 -

Business Continuity and Disaster Recovery Planning

MIS5206 Week 8

- Team Presentation
- Mid-term Review
- Week 7 Material Review
- BCP/DRP
- Test Taking Tip
- Quiz

MIS5206 Week 8

- Team Presentation
- Mid-term Review
- Week 7 Material Review
- BCP/DRP
- Test Taking Tip
- Quiz

In the News

Hackers strike defense companies through real-time ad bidding

Online Security and Risk - A major change this year in how online advertisements are sold has been embraced by hackers, who are using advanced ad-targeting capabilities to precisely

Security vendor Invincea said it has detected many instances of people within defense and aerospace companies stumbling across malicious advertisements that are shown only to them, a scheme it calls "Operation DeathClick."

Reading

- Vacca Chapter 36
- ISACA Assignments:
  - ISACA Assignment 1: “Disaster Recovery and Business Continuity Planning: Testing an Organization’s Plans” http://www.isaca.org/Journal/Past-Issues/2002/Volume-1/Pages/Disaster-Recovery-andBusiness-Continuity-Planning.aspx
  - ISACA Assignment 2: “What Every IT Auditor Should Know About Backup and Recovery” http://www.isaca.org/Journal/Past-Issues/2011/Volume-6/Pages/What-EveryIT-Auditor-Should-Know-About-Backup-and-Recovery.aspx

Business Continuity and Disaster Recovery Planning

Operating disruptions can occur with or without warning. The results may be predictable or unanticipated. It is important that the mission of the enterprise is sustained during any emergency. The first priority is always the safety of the people: Employees, Service and Support Staff and Visitors.

Business Continuity
- versus -
Disaster Recovery

Business Continuity Planning	Planning for the purpose of developing a "Roadmap" for continuing operations under adverse conditions after a natural or human-induced interruption
Disaster Recovery Planning	Planning in preparation for recovery or continuation of technology infrastructure critical to an organization after a natural or human-induced disaster

Business Continuity Planning

- Business continuity planning is about maintaining, resuming, and recovering the business, not just the recovery of the technology
- The planning process should be conducted on an enterprise-wide basis
- A thorough business impact analysis and risk assessment are the foundation of an effective Business Continuity Plan.
- The effectiveness of a BCP can only be validated through testing or practical application.
- The BCP will be updated at least annually to reflect and respond to changes in the financial institution or its service provider(s).

BCP Process

- Project Initiation & Management
- Business Impact Analysis (BIA)
- Recovery Strategies Development
- Plan Design & Development
- Testing, Maintenance, Awareness, Training

… Repeat

Project Initiation & Management

- Often overlooked as a key part of the BCP process
- Allows for a consistent, repeatable approach
- Provides a way to make sure there is Executive Sponsorship and visibility
- Considered a Best Practice

Business Impact Analysis (BIA)

- Differentiates critical (urgent) and non-critical (non-urgent) organization functions/activities
- Identifies Critical functions are those whose disruption is regarded as unacceptable
- Impact scenarios are described and quantified
- Priorities are developed in light of the the cost of scenarios recovery solutions

Recovery Strategies Develop

- Approaches to “re-initiate” crucial business functions and resume on-going operations are developed and documented
- Execution strategies, resources, timelines and dependencies are documented
- Strategies are confirmed and reviewed by function owners in the business as well as executives

Plan Design & Development

- Recovery Strategies Scenarios are integrated and synchronized
- Formal Plan document is created
- Stakeholder review and sign-off on the plan

Testing, Maintenance, Awareness, Training

- Testing is the ONLY way that a plan can be assessed for effectiveness
- Testing can be expensive and must be prioritized with high level sponsorship
- This requires an ongoing commitment by the business as the plan must be re-assessed on a regular basis

Disaster Recovery Planning

- Establish a planning group
- Perform risk assessment and audits
- Establish priorities for applications and networks
- Develop recovery strategies
- Prepare inventory and documentation of the plan
- Develop verification criteria and procedures
- Implement the plan

Computer Operations

Areas of Focus:

- Sites/ Locations/ Facilities
- Computers and Infrastructure (Hardware)
- Operating Systems
- Applications (software)
- Data
- Supplies
- Documentation
- Personnel

Application Systems

Classification of Applications*

Classification		Description
1	Mission Critical	Mission Critical to accomplishing the mission of the organization Can be performed only by computers No alternative manual processing capability exists Must be restored within 36 hours
2	Critical	Critical in accomplishing the work of the organization Primarily performed by computers Can be performed manually for a limited time period Must be restored starting at 36 hours and within 5 days
3	Essential	Essential in completing the work of the organization Performed by computers Can be performed manually for an extended time period Can be restored as early as 5 days, however it can take longer

* From SANS

Audit Focus Areas

Areas for audit evaluation:

Figure 3—Possible Tests/Procedures for Backup and Recovery	
Data	• Review or observe backup procedures. • Review documentation of a successful restore (within the last year). • Verify restoration personally (when risk is high or restoration is an audit objective).
Site/computers/ OS	• Review the provisions of the BCP/DRP. • Review a contract (hot site, cold site, mutual aid, etc.). • Verify the ability to restore these aspects.
Applications	• Review the plan's provisions. • Review the critical applications list, including ranking. • Verify the ability to restore (personally, when risk is high or restoration is an audit objective). • Observe or inquire about the backups of application software and location.
Supplies/ documentation	• Review the plan's provisions. • Observe or inquire about the provisions and location.
Recovery team	• Review the plan's provisions. • Interview one or more members of the team, and ask about roles and responsibilities. • Gain assurance that there is provision for adequate personnel for a successful restoration.

DRP Testing Approaches

- Conducting a structured walk-through
- Conduct Dry-Run tests
  - Can be conducted on a function by function basis
  - Do not have test all functions for each cycle
  - Tests should involve actual interruptions and recoveries
- A tracking matrix should be created and maintained to track performance across multiple periods
- Business Process changes must be tracked and specific test scenarios created to ensure the existing recovery processes will support the new scenarios
- Test should demonstrate and document that roles are clearly defined and understood

Test Taking Tip

Don't Revise Your Answer

(without a very strong reason)

- Your first answer is probably the right one
- On an exam where there is no penalty for wrong answers, you are just using time that might have gone to getting another correct answer
- If you are having second thoughts, plan to come back to that question after you have completed the entire test

Quiz