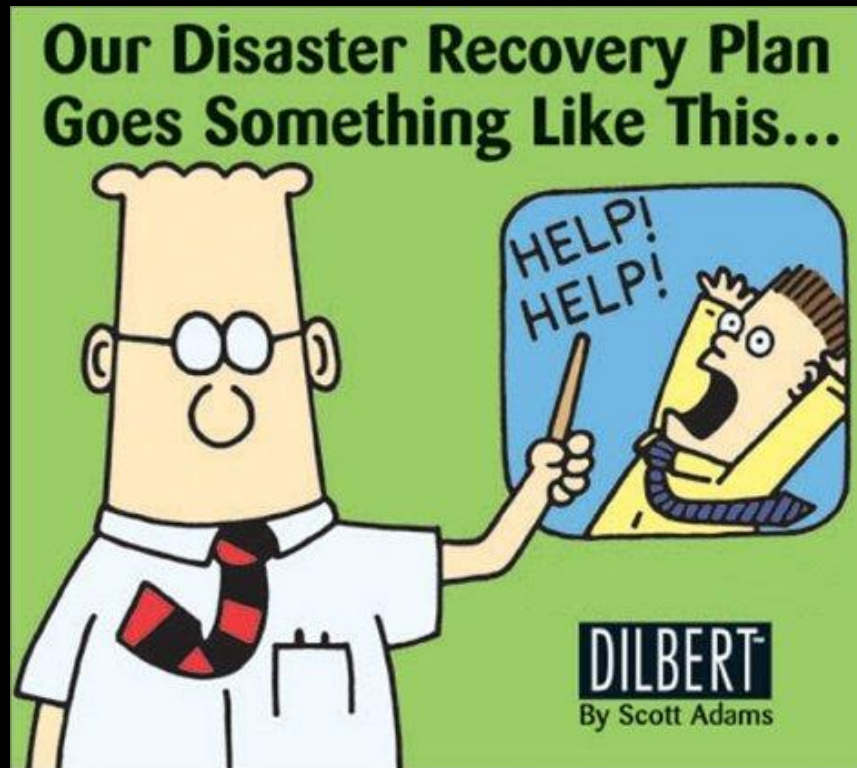


A Practical Guide to Business Continuity & Disaster Recovery

*Keith A. Conlee – CISSP,
CBCP*

*Chief Security Officer
Information Technology*

The Plan



The Plan - continued



Business Continuity vs. Disaster Recovery

- Many definitions provide much confusion about the terms
- I prefer “Business Continuity Management”
 - Defines holistic management processes that identify potential impacts that threaten an organization and provides a framework for building resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, and value creating activities.

Business Continuity Management

- The Primary Objective
 - To allow business operations to continue under adverse conditions, by the introduction of appropriate resilience strategies, recovery objectives, business continuity and crisis management plans in collaboration with, or as a key component of, an integrated risk management initiative.

Introduction & Overview

- Use a Methodology
- DRI International and the BCI based in the UK
- Contractors / Consultants may use something different – developed in-house
- Vendor supplied – usually with planning software, e.g. Strohl Systems, Coop Systems

About DRII

- Founded in 1988 as the Disaster Recovery Institute in order to develop a base of knowledge in Continuity Planning and the Management of risk
- DRII administers the industry's premier educational and certification programs for those engaged in the practice of BC planning and management.
- More than 3100 individual's world-wide maintain professional certification through DRII.

Common Body of Knowledge

- Developed by recognized experts in BC/DR planning and education
- Provides a resource base and guide for BC / DR professionals / technicians from which to develop BCPs for their own institutions

Common Body of Knowledge (cont.)

- Project Initiation and Management
- Risk Evaluation and Control
- Business Impact Analysis
- Developing Business Continuity Strategies
- Emergency Response and Operations

Common Body of Knowledge (cont.)

- Developing and Implementing Business Continuity Plans
- Awareness Programs and Training
- Maintaining and Exercising the Business Continuity Plans
- Crisis Communications
- Coordination with External Agencies

Project Initiation and Management

- Establish a need for BC/DR planning
 - Identify the value-added
- Must get support of upper management to be successful
- Business Impact Analysis (BIA) will play a big role (discussed in a few slides)

Risk Evaluation and Control

- Determine what business interruption events (risk) and the probability of each that can adversely affect your organization and what controls are currently in place to eliminate or mitigate each risk.
 - FEMA site - natural disaster
 - Facilities Mgr / Risk Mgr - “non” natural disaster
 - Network Mgr – virus / spyware / “phishing” like trends

BC / DR Plan Must Haves

- Unlimited Budget
- Unlimited Resources
- Scapegoat

Business Impact Analysis (BIA)

- What is it
 - Estimates the financial and operational impact all credible disruptive events would have on your day-to-day business. It also identifies critical processes/applications/systems, the people who use and support them, and the risk tolerance for each. The BIA allows you to define the target of your BC/DR Plan.

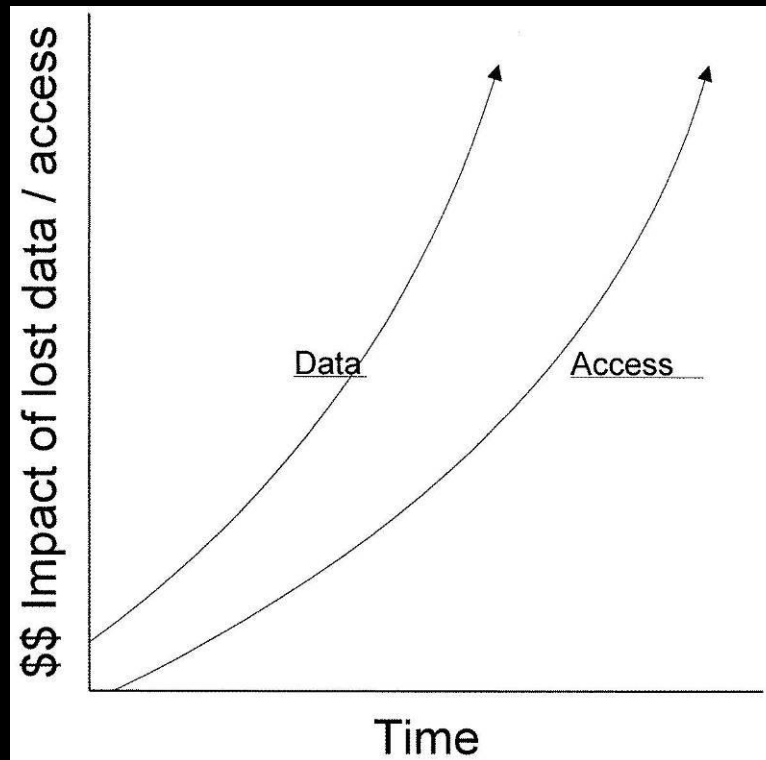
(BIA) - continued

- Identifying your BC/DR Plan Target
 - Locate and identify key stakeholders
 - Identify and prioritize critical applications & data
 - Identify the impact (in \$\$\$) of the loss of critical applications & data over time.
 - Identify the level of risk assumption for each critical application and data

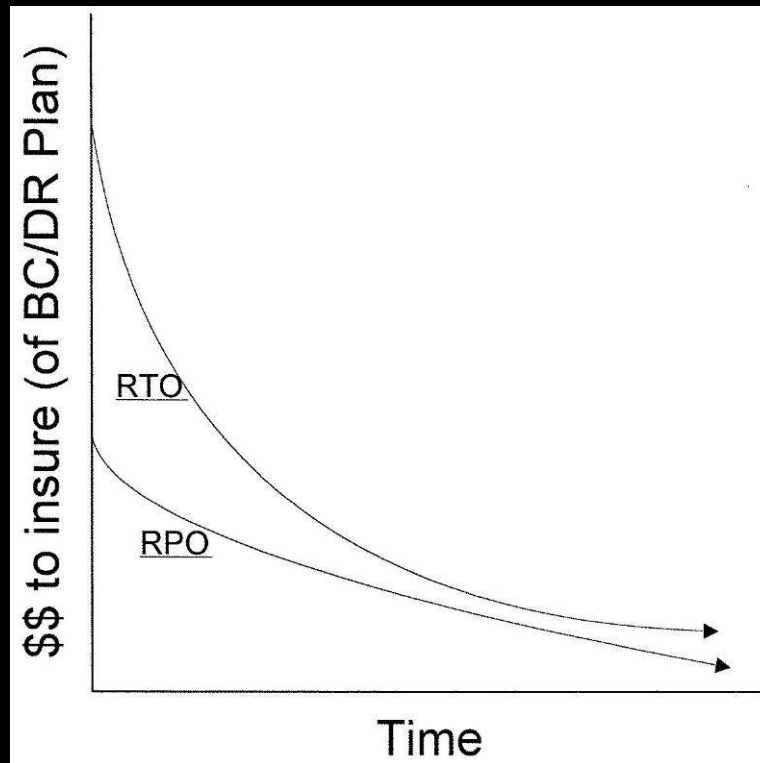
(BIA) - continued

- Identifying your BC/DR Plan Target - continued
 - Identify the “Recovery Time Objective” (RTO), i.e., the maximum amount of time allowed without access to each critical application & data.
 - Identify the “Recovery Point Objective” (RPO), i.e., the maximum amount of data loss (usually measured in time) allowed for each critical application.
 - RTO and RPO can be put on a time vs. \$\$ business impact sliding scale, and a time vs. \$\$ BC/DR cost sliding scale (see examples following)

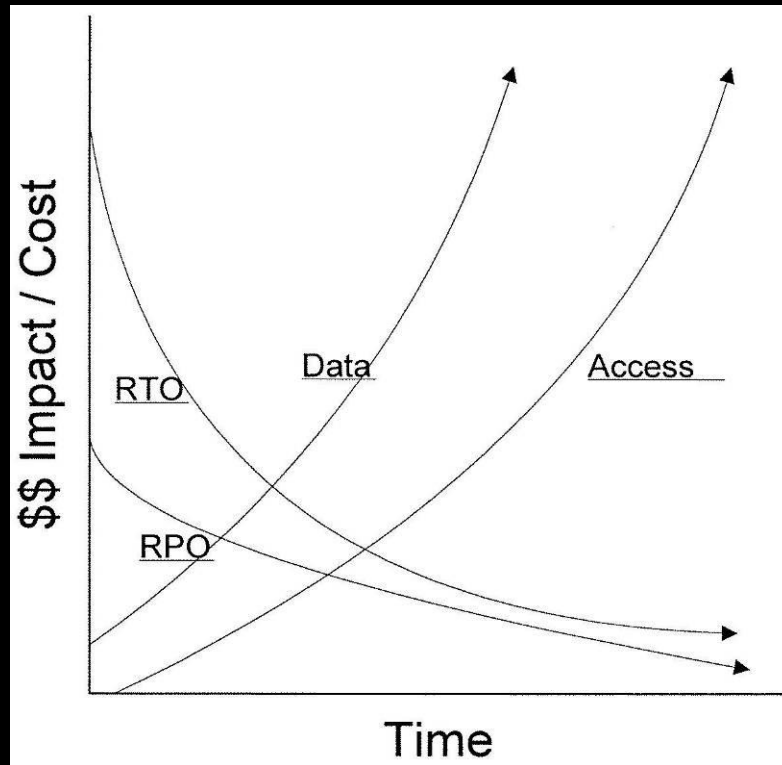
(BIA) - continued



(BIA) - continued



(BIA) - continued



(BIA) - continued

- Quantifying \$ Impact
- “Annualized Loss Exposure”
$$\text{Risk} = \text{Frequency/yr} * \text{Exposure}$$
- Example – Power Failure
$$\text{Risk} = 5/\text{yr} * \$2000/\text{Pwr Failure}$$
$$\text{Risk} = \$10000/\text{yr}$$

Developing Business Continuity Strategies

NOW THE FUN BEGINS!

- People and Safety issues always come first
- Document the scope of your plan and the assumed risks. Remember you can never eliminate all risk.
- Define and Identify teams and the team hierarchy
- Define a notification sequence of the teams

Developing Business Continuity Strategies - continued

- Identify the technical infrastructure (h/w & s/w) that supports each critical application in “the plan” and any pre-positioned resources that may be required – remember RTO
- Define a backup and off-site scheme for all critical application data and identify resources that maybe be required to meet your RPO.

Emergency Response and Operations

Notification Sequence

- Who pulls the trigger – “any business interruption that can not be handled by normal operations procedures” should be evaluated as a reason to execute your BC/DR Plan.
- Alternative Command Centers
- What kind of notification system(s) will you use?
- Who gets notified first, second, etc.

Emergency Response and Operations - continued

- Example notification sequence/breakdown
 - Disaster Management Team - first
 - Disaster Assessment Team – second (get pre-event clearance)
 - Technical team (on-alert vs. declared disaster)
 - Local police and medical team (make sure they know about your plan)
 - Executive Team

Emergency Response and Operations - continued

- Example notification – continued
 - Pre-positioned recovery services providers
 - Public Relations Team
 - User Management (stakeholders)
 - Vendor Team

Developing and Implementing Business Continuity Plans

FILL IN THE DETAILS!

- Assign team members and backups
- Define a notification sequence with actual names
- Identify in detail the technical infrastructure (h/w & s/w) that supports each critical application in “the plan” and the staff & backups who will recreate it if the plan is executed – remember RTO

Developing and Implementing Business Continuity Plans - continued

- Secure required resources for any identified pre-positioned infrastructure/services to meet RTO/RPO
- Implement a backup schedule / and off-site scheme for all critical application data that will meet your RPO.
- Have support teams write step-by-step procedures for recovering the different technical infrastructure pieces, e.g. h/w, OS, critical apps s/w, data

Developing and Implementing Business Continuity Plans - continued

- Define operation procedures (if different) once “recovery” is complete.
- Develop your Test Plan
- Develop your Maintenance Plan

Awareness Programs and Training

- Define Awareness and Training Program
- Create and maintain institutional awareness
- Create and maintain training program for all team members and their backups.

Maintaining and Exercising the Business Continuity Plans

Maintaining Your Plan

- Define review periodicity
- Maintain good change control procedures
- Keep good inventories
 - h/w (ser. #s), s/w levels/keys, firmware versions, etc.
- Password / Identity management – root/admin

Maintaining and Exercising the Business Continuity Plans - continued

Exercising / Testing Your Plan

- Without exercising/testing – you do not have a plan
- Establish a Program for exercising/testing
 - E.g., types of tests, periodicity, reporting, etc.
- Define success criteria (remember RTO, RPO – and use your stakeholders)

Maintaining and Exercising the Business Continuity Plans - continued

- Use the results to build on strengths and improve weak areas.
- All exercises and tests are good regardless of results.
- Use the results to update your Plan as needed

Crisis Communications

- How do you communicate internally?
 - Includes team members, employees, management, customers (stakeholders), vendors, suppliers, and the media
 - What kind of notification system(s) to use?
 - Must be exercised!

Coordination with External Agencies

- Become familiar with the Incident Command System (ICS) in your area.
- Make sure ICS knows about you (get pre-event clearance for DAT)
- Many ICS groups will review your BC/DR plan/strategy (this usually makes their jobs easier)
- Maintain current knowledge of laws and regulations concerning Emergency Management

Summary

- BC / DR Planning is all about making as many decisions (pre-event) as possible in a calm and thoughtful manner for a time (post-event) when chaos will rule and time is of the essence.
- Thanks

QUESTIONS ???

Keith Conlee – CISSP, CBCP

Chief Security Officer, IT

College of DuPage

425 Fawell Blvd.

Glen Ellyn, IL 60137-6599

conlee@cod.edu