BCP DRP DEVLOPMENT

By

Yulhendri

Session's Agenda

- Introducing Business Continuity (BC) and Disaster Recovery (DR)
- Commencing Business Continuity Lifecycle and Activities
- Defining Business Continuity Universe
- Conducting Business Impact Analysis

Session's Agenda (cont'd)

- Defining Resumption Planning
- Communicating and Socializing BCP
- Training and Testing BCP
- Implementing and Monitoring BCP
- Reviewing and Updating BCP
- Post Test
- Wrapping-Up and Closing

INTRODUCING BUSINESS CONTINUITY (BC) AND DISASTER RECOVERY (DR)

What BC Addresses

- How to continue doing business until recovery is accomplished
- How to restore core businesses operations when disasters occur
- Continuation of critical business processes when a disaster destroys data processing capabilities
- Preparation, testing and maintenance of specific actions to operate like normal processing

Scope of BC

- Used to be just a data center
- These days, it includes:
  - Operational activities
  - Personnel, networks, infrastructures
  - All aspects of IT environment: policies, processes, procedures, hardware, software

BC Main Objectives

Create, test, monitor, review and update a plan that will:

- Allow timely resumption of critical business operations
- Indirectly allow timely recovery of critical business operations and furthermore non-critical business operations (DR domain)
- Minimize loss (human safety and assets)
- Meet legal and regulatory requirements

BC Major Objectives (cont'd)

According to The Institute of Internal Auditors (IIA) www.theiia.org:

- Availability as the main focus (critical business processes)
- Confidentiality of the company (tangible and intangible assets)
- Integrity of data and information

BC Responsibilities

General Business

- First responder: Evacuation, fire, health…
- Damage Assessment
- Emergency Mgmt
- Legal Affairs
- Transportation/ Relocation/Coordination (people, equipment)
- Supplies
- Salvage
- Training

IT-Specific Functions

- Software
- Application
- Emergency operations
- Network recovery
- Hardware
- Database/Data Entry
- Information Security

Contact information is important!

How to Develop BCP

- It's an on-going process, not a project with a beginning and an end
  - Creating, socializing, training, testing, monitoring, controlling, reviewing and updating
  - "Critical" business functions may evolve
- BCP team must constitute both business and IT personnel
- Requires support from top management and executives

BCP Responsibilities

Focus	IT	Business
Event Resumption	Resumption Plan Procedures to resume at secondary/temporary site	Resumption Plan Procedures to resume business operations at secondary/temporary site
	IT Contingency Plan: Recovers major application or system	Emergency Response Plan Protect life and assets during physical threat
	Cyber Incident Response Plan: Malicious cyber incident	Crisis Communication Plan Provide status reports to public and personnel
Business Continuity		Business Continuity Plan
		Continuity of Operations Plan Longer duration outages

Defining Disaster

Imagine an organization:

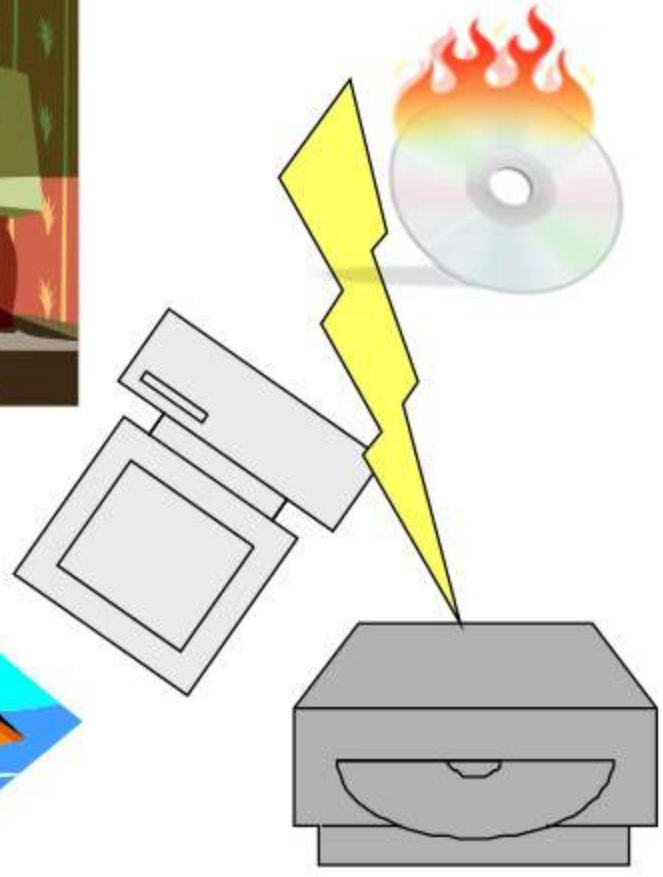
- Bank with 50 million accounts, social security numbers, credit cards, loans…
- Airline serving 60,000 people on 300 flights daily…
- Pharmacy system filling 15 million prescriptions per year, some of the prescriptions are life-saving…
- Factory with 2000 employees producing 500,000 products per day using robots…

Defining Disaster (cont'd)

Imagine a failure like

- Production server failure
- Transaction Disk System failure
- Hacker break-in
- Extended power failure
- Tsunami
- Spyware
- Malevolent virus or worm
- Earthquake, tornado
- Employee error or revenge

How will this affect each business?



What DR Addresses

- Should be oriented towards recovering AFTER the DISASTER.
- Focus more into how organizations could get fully recovered into their normal level of all of their business processes.

Contents of DRP

- Pre-incident readiness
- Evacuation procedures
- Identifying persons in charge, contact information (SW and HW vendors, insurance, recovery facilities, suppliers, offsite media, human relations, law enforcement)
- Step-by-step procedures
- Required resources for recovery operations

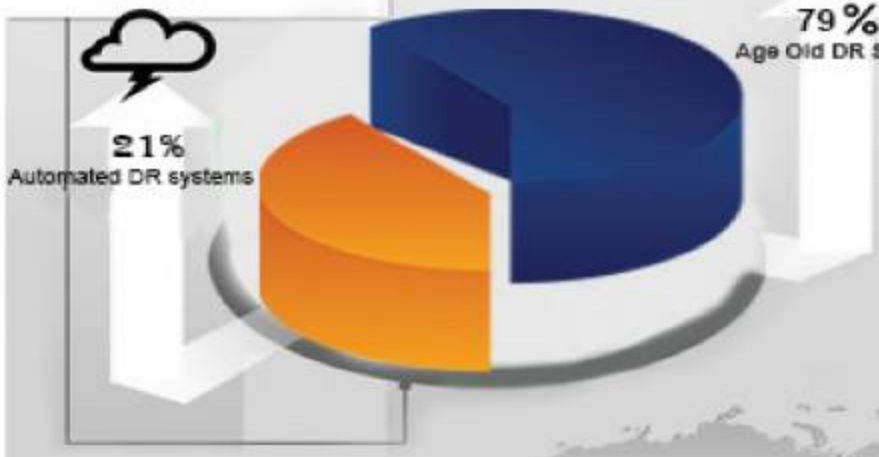
Trends in Disaster Recovery

1

Automated DR systems are being used by only 21% organizations These 21% use highly available system with Data replication

2

The remaining 79% use other backup forms and technologies like Disc Backup, Tape Backup, etc.

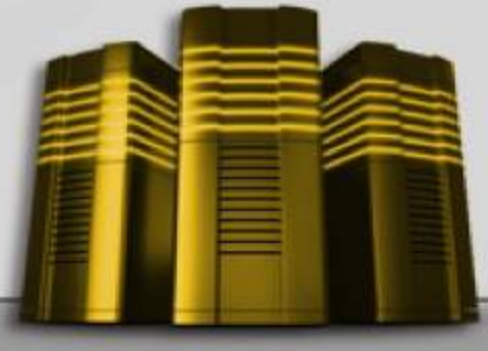


ConsolePark Disaster Recovery Solutions help you in...

- Instant Data Restoration
- Automated DR Systems
- Efficient Data Replication
- Avoiding Data Loss

Why Automated Disaster Recovery ??

- To avoid errors occurring due to manual processing that leads to data loss and declined productivity
- Approx 65% companies rely on manual DR processing.
- Around 42% have past data loss experiences
- 67% companies believe data loss hampers productivity .



Source : IDG Research Services

Forrester Says on DR

1

MYTH:
We can deliver a better recovery capability if we keep DR in our own data center

FACT:
Research shows that confidence may not match reality

59%

of firms were **only somewhat successful** in meeting recovery objectives during testing

34%

are **not sure they could respond** to a real disaster

2

MYTH:
We have the resources to support an in-house DR plan

FACT:
Keeping DR on the path of continuous improvement is hard

52%

of firms of firms face a **lack of focus** on in-house DR relative to other IT projects

6.2%

of **IT budgets on average** go to business continuity and disaster recovery

Forrester Says on DR (cont'd)

3

MYTH:
Insourcing DR costs less than outsourcing, so funding won't be an issue

FACT:
Beware of hidden costs related to technology refreshes and systems management

38%

of firms **struggle against lack of funding** to keep DR infrastructure up to date

31.1

full-time employees support business continuity management corporatewide[2]

4

MYTH:
We have the skills we need to protect our data and business processes

FACT:
Expertise is essential to effective DR—and not easy to come by

34%

of do-it-yourselfers **lack adequate in-house DR skills**

Forrester Says on DR (cont'd)

5

MYTH:
With DR under our control, we can do a better job of testing

FACT:
Testing is too often the victim of conflicting priorities

48%

of do-it-yourselfers have **trouble running enough DR tests** and exercises

5%

have **not run a single test** or exercise **in over a year**

Do-it-yourself or outsource?

It's not an "all or nothing" choice

Forrester Says on DR (cont'd)

57% of survey respondents source DR capabilities with an equal mix of in-house and outsourced resources

What would make you consider outsourcing part or all of your DR?

Survey respondents want providers to offer:

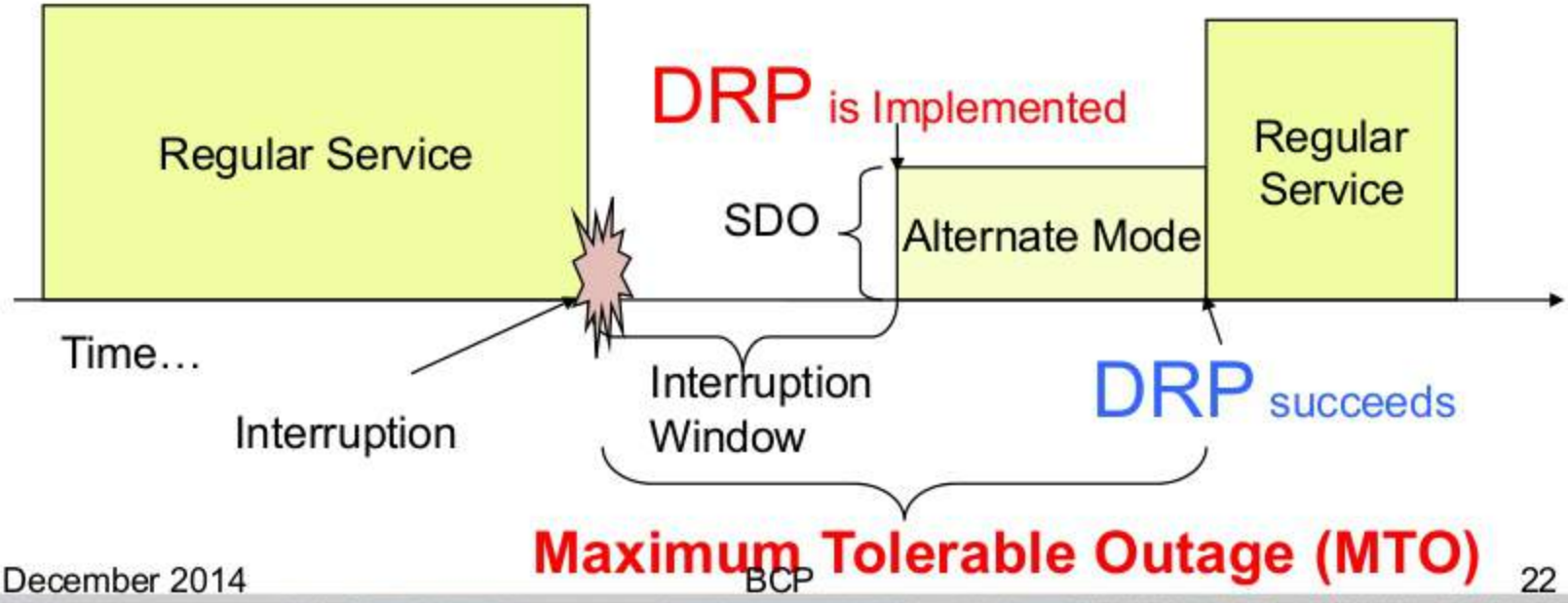
Better TCO for outsourcing over in-house	56%
A portal for real-time testing or failover	43%
Help with the transition to service provider	40%
Flexible contract terms	36%
A mix of traditional and cloud-based DR	35%

Where BCP and DRP Fit In

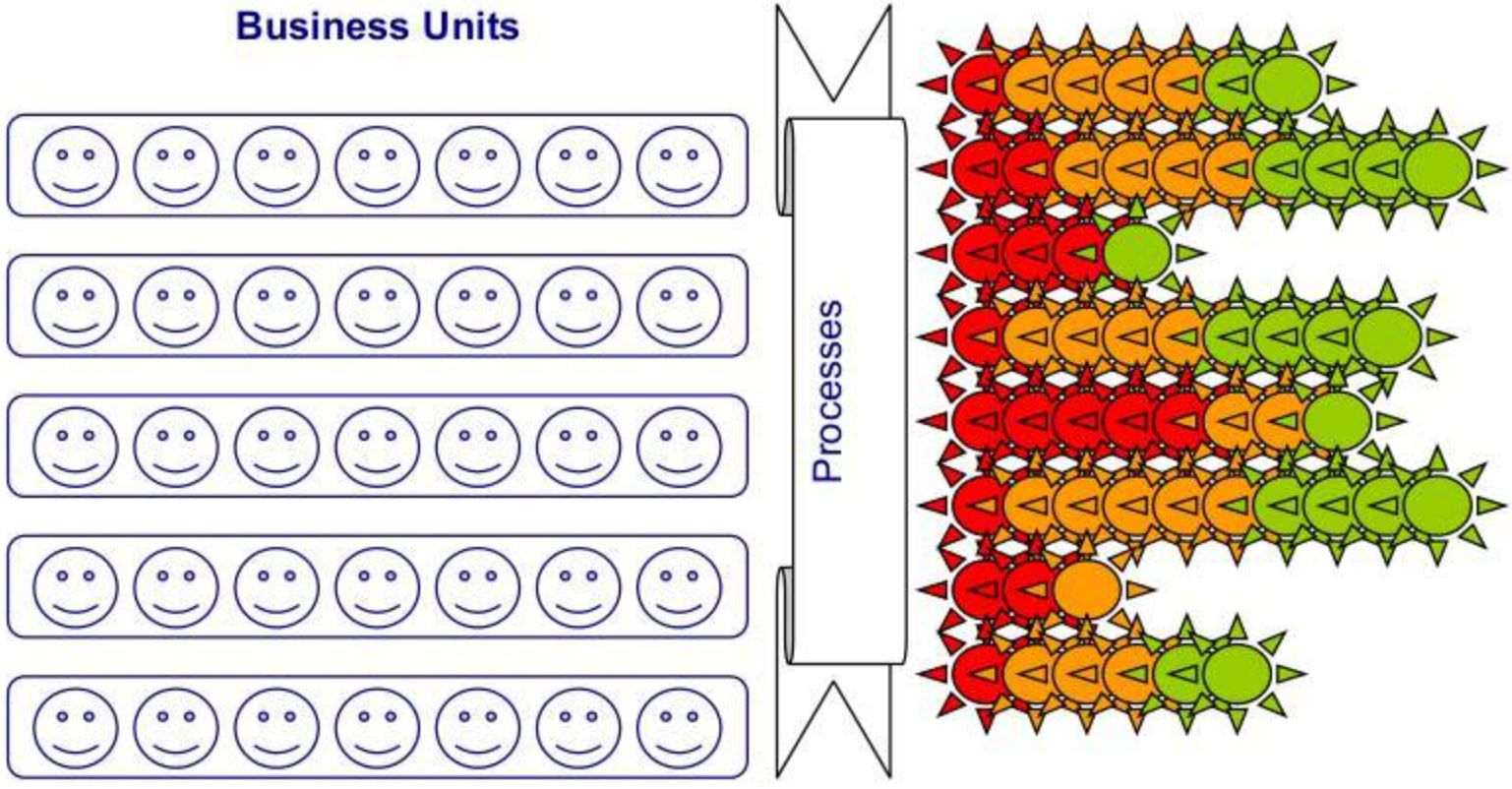
Interruption Window: Time duration organization can wait between point of failure and service resumption

Service Delivery Objective (SDO): Level of service in Alternate Mode

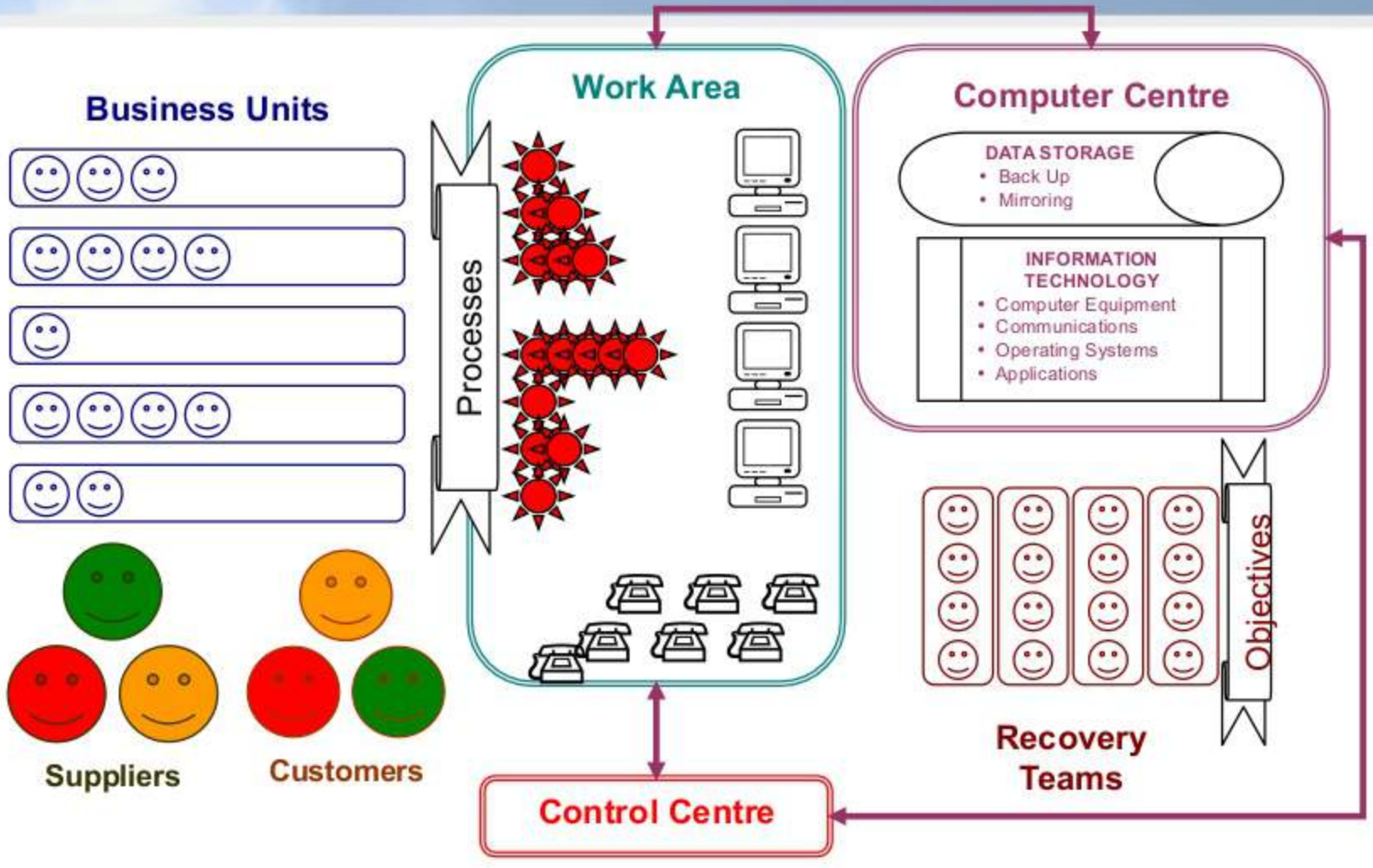
MTO: Max time in Alternate Mode where **BCP** take its role



BC AND DC: Normal Operations



BC AND DC: Solution



Concerns for BC and DR

- Evacuation plan: **People's LIVES** always take **FIRST priority**
- Disaster declaration: Who, how, for what?
- Responsibility: Who covers necessary disaster recovery functions
- Procedures for Business Continuity
- Procedures for Alternate Mode operation
  - Resource Allocation: During recovery & continued operation

    Copies of the plan should be off-site