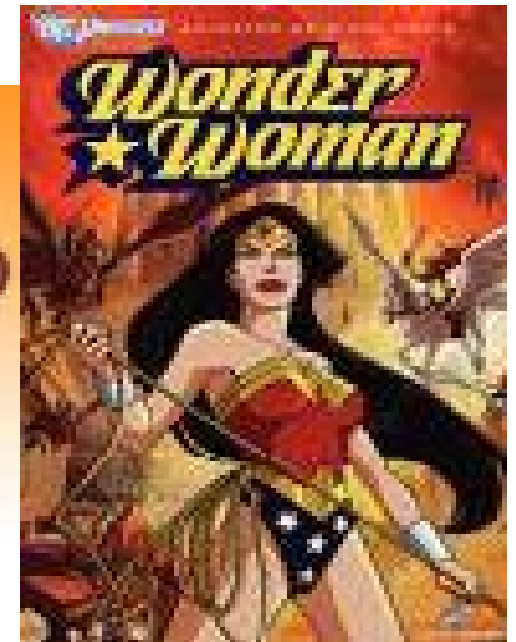


Lessons Learned

Living outside the box

Presented by: Becky Cohen, C.B.C.P.
a/k/a *the disaster diva*

Evolution of business continuity



Definition

- Planning to ensure the continuation of operations in the event of a catastrophic event.
- Business continuity planning includes the actions to be taken, resources required, and procedures to be followed to ensure the continued availability of essential services, programs, and operations in the event of planned and unplanned interruptions.



Bottom line



Companies are faced with disasters of varying severity everyday. Those that have meaningful plans in place to deal with them will survive, those that don't, may not.

In the last 45 days:



In the past 45 days



Well Known Disasters

Often those affected escaped the actual disaster damage

- Oct 17, 1989 – San Francisco Earthquake
- April 13, 1992 – Chicago Flood
- Apr 19, 1995 - Alfred P. Murrah Federal Building Bombing
- Sept 11, 2001 – World Trade Center
- August 25, 2005 – Hurricane Katrina *

Not All Disasters are Richter Scale 8, DHS Level Orange, or 6 o'clock news worthy

Most outages are the result of more common events

- Hardware Failures
- Power Failures
- Water Leaks
- Fires
- Human Error



Can You Afford Not to be Prepared?

Consider these facts:

- 93% of companies that lost their data center for 10 days or more due to disaster filed for bankruptcy within a year. 50% that were without a DRP filed immediately (Source: National Archives and Records Admin – Washington)
- Company survival in doubt after the % of downtime:
 - 4% in the hour, 3% in 1 hour, 9% in 4 hours, 15% in 24 hours, 21% in 48 hours, **40% in 72 hours**....(Source: 2001 Cost of Downtime Survey Results, 2001.)

Closer to home; what would happen in your environment if you lost....

- Consider – Impact of Email Loss
- Consider – Impact of Accounting Application
- Consider – Impact of Loss of Fileserver
 - *The financial impact of downtime and data loss staggering. The cost of data loss not only dollars and downtime, but also productivity*



Are You at Risk?

Take a Look Around

- Environmental
 - Is it too hot? Too humid?
 - Where is your computer center located?
- Power
 - Do you have backup power supplies?
- Data Protection
 - Disk Redundancy ?
 - Is your data backed up?

Cover Your Assets. Start Small but Start Now

- Prevention
 - Physical Security, UPS, RAID
- Identify What is Important
 - Critical databases, application data, email, file servers
- Back it Up!
 - Establish a backup strategy
 - Full, incremental, differential
- Test recovery, then test it again

What is a Disaster Recovery Plan?

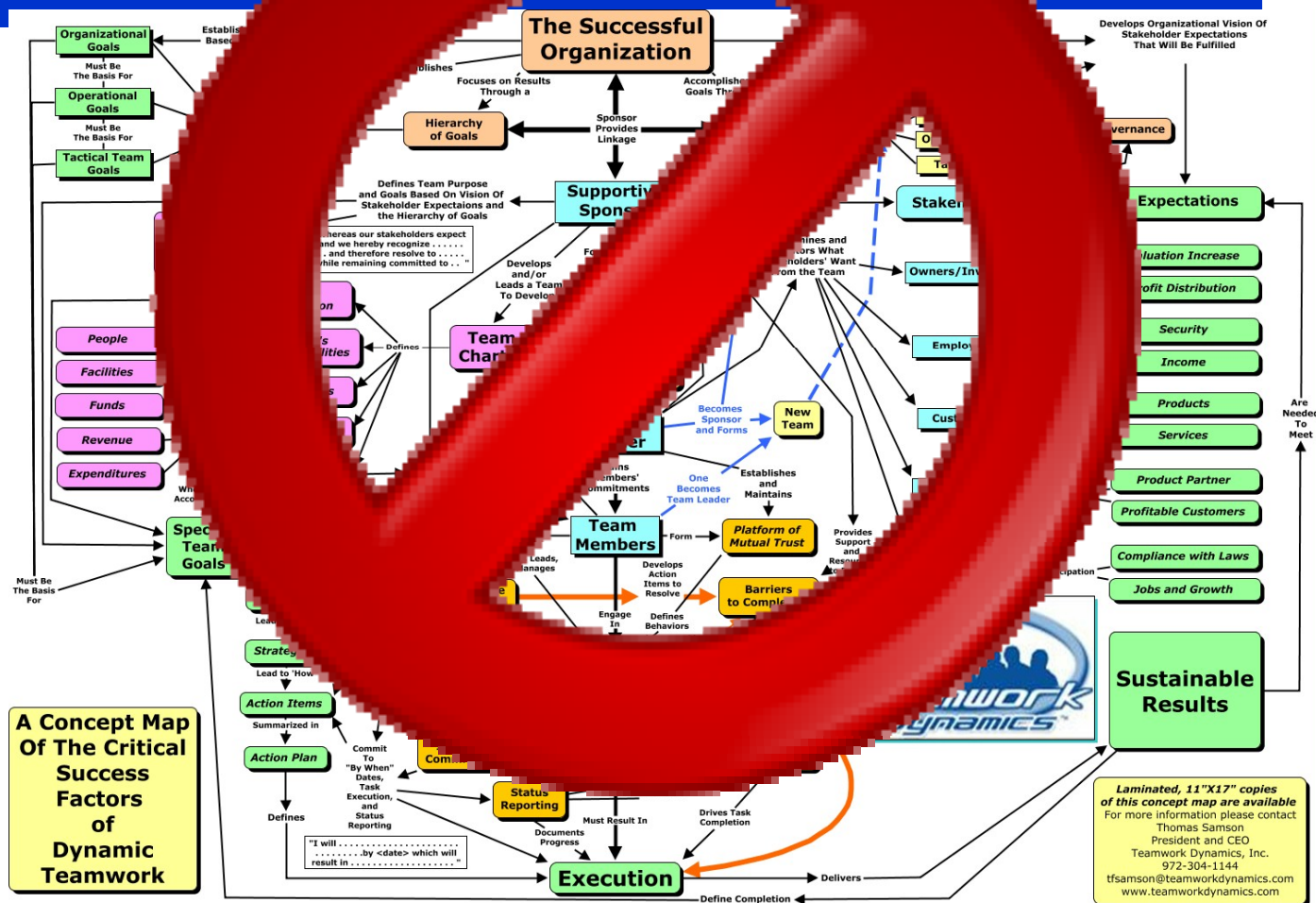
- It is the most important tool in your arsenal in the event of a disaster or serious incident
 - Difference between survival and loss of your business
 - Preparation for the unexpected
 - Documented series of steps an organization must take to recover services



Disaster Recovery Plan Goals

- Prevention
 - Protect the organizations assets and manage risk
- Response
 - Policies, procedures and actions to be followed in the event of an emergency
- Resumption
 - Resumption of only the most time-sensitive business operations immediately following a disaster
- Recovery
 - Implementing expanded operations to address less time-sensitive business operations immediately following an interruption or disaster
- Restoration
 - The repair or relocation of the primary site and its contents and for the restoration of normal business operations at the primary site

Creating a Business Recovery Plan



Creating a Disaster Recovery Plan

- Have Executive approval and 'buy-in'
- Risk Analysis
 - Identify threats and risks
 - Rate probability and impact – Low, Medium or High
- Establish the Budget
 - Cost of prevention
 - Business input critical
 - 2-8% of IT budget - Typical rule of thumb

Creating a Disaster Recovery Plan

- Develop the Plan
 - Crisis Management Procedures
 - Recovery priorities
 - Recovery teams and responsibilities
 - Detailed recovery procedures or “scripts”
 - Contact lists – vendors, employees
 - Verification Checklists
- Test, Test, Test
- Review and Maintain



What have we learned from recent events?

- EXPECTATIONS

- Reset your **scale of devastation**
- **Self-reliance!** Power, communication, supplies
- **Access** is not always guaranteed
- **No mail** service
- **Be flexible** and improvise
- ***Do the work now!***

Are you prepared?

- Be creative to solutions
- Address unforeseen difficulties quickly
- Don't just focus on I.T.
- It's about the PEOPLE!
 - And recovering from all levels of the organization
- *3 must haves*

How much planning /preparing is enough?

- You cannot prevent or anticipate disasters
- Practice, Test, Drill, Rehearse
 - Build confidence
 - Identify potential threats
 - Assess impact
 - Assign priorities
 - Develop planned responses
 - Include all critical functions and areas
- ***Make it a 'corporate culture'***



How thorough should testing be?

- Disaster drills need to be relevant
- Disaster drills should simulate realistic disasters
- Test to standard volumes, and all types of transactions
- Include worst case scenarios
- *Back to basics*

Lessons Learned -

- Anticipate disruptions in communication services, possibly for an extended period of time
- Critical staff may not be able to reach their assigned post or location
- Replacement supplies may be difficult to obtain during a protracted recovery period
- Back up sites and your own/brick and mortar
- People are essential

Summary

- Disasters vary in severity, but the impacts can be life threatening to a business
- The costs of unplanned outages can be financially crippling
- A *simple* plan is far superior than no plan at all
- The goals of DR are prevention, response, resumption, recovery and restoration
- *...it's about the people!*





Questions?



- *Any questions, please feel free to contact me*
- Becky Cohen, CBCP
- 954-940-5688
- bcohen@bankatlantic.com



Questions?

