

Disaster Recovery and Business Continuity
“A technology-based, General Business Discussion”

www.datachambers.com

PROPRIETARY and CONFIDENTIAL

1



Inside the Numbers

- ❑ **93% of organizations that lose critical systems for more than 10 consecutive days file bankruptcy almost immediately**
- ❑ **90% of companies that experience a catastrophic loss of data and equipment without a disaster recovery plan are out of business within 2 years.**
- ❑ **52% of U.S. companies have had business operations significantly interrupted because of computer hardware problems**



Inside the Numbers

- ❑ **1 in 5 companies will suffer a serious business interruption in the next year, which will result in an organization having to cease operations for a period of time -ATT**
- ❑ **Companies that plan for a possible business interruption, by utilizing a tested plan, increase their chance of survival by 70% over those who do not have a plan. -FEMA**



Business Interruption: The Myths

- “Only big businesses need a plan”**
- “My IT staff takes care of that”**
- “DR plans are too expensive”**
- “Our company has insurance for that”**
- “We have great employees....they will know what to do”**
- “Our company is not required to have a DR plan”**
- “We can work from home”**
- “Our customers are very loyal”**



Current Events

“Business interruption” threats

Currently in the news:

- Power interruptions more frequent
- Network outages common
- Mail threats and corrupt data more prevalent
- Computer crimes the “new norm”
- Terrorism now a fact of life
- Unpredictable weather (warming, etc.)
- Water shortages (health department can shut you down)
- M1H1 and Avian Flu cases increasing
- California fires could happen here



Here is what we'll discuss

- ✓ **Business Continuity Basics**
- ✓ **Threats and Hazards**
- ✓ **The Planning Process**
- ✓ **Current BC and DR Trends**
- ✓ **Budget/Cost**
- ✓ **Q & A**



Business Disaster

A ***Business Disaster*** is not a fire, tornado, hurricane, flood, etc. Those are the ***causes***.

A ***Business Disaster*** is that point in time, after the ***cause***, when your business **cannot** provide your customers and users with the minimum level of service they both need and expect!



Business Continuity Basics

- Disaster Recovery vs. Business Continuity
- What is an effective Plan?
- What does a Plan Include?
- Who needs a Plan?
- Why have a Plan?
- How to get started?



DR vs BC

❑ Disaster Recovery

Takes action AFTER service interruption

- Tape/Electronic backup
- Cold/Warm equipment or site

❑ Business Continuity

Proactively avoids service interruption

- Clustered equipment
- Hot/Mirror equipment or site



Why have a Plan ?

- Keep clients / Retain customer base**
- Protect your business from extinction**
- Business Continuity Practices can actually save you money**

“It’s the little things!”

Small service outages averted add up to big money saved

- Instills a discipline within an organization**
- Government regulations**



Who needs a Plan?

- ❑ **Any company guaranteeing a minimal service level or product to their end customer**
- ❑ **Public Companies / Financial Companies**
- ❑ **Any company or organization who must have ongoing access to mission critical data**
- ❑ **Any business that if they are unable to conduct business for several hours or days could cause them to go out of business**
- ❑ **Professional service firms: Legal, Accounting, Insurance and Financial Services**



What is an effective Plan?

An effective plan is one that

- ✓ **Meets current legislative requirements**
- ✓ **Meets current industry best practices**
- ✓ **Allows you the ability to continue providing a minimum level of service or product shipment to your end consumer given any type of business interruption.**



What does a Plan Include?

- ✓ **An effective documented Business Continuity Plan**
- ✓ **Data backup and restore plan**
- ✓ **Employee notification plan**
- ✓ **Work Force recovery area**
- ✓ **Computer processing contingency**



Principles of Emergency Management

❖ Awareness

- ✓ Activities to identify what could happen
- ✓ Threats, hazards, vulnerabilities

❖ Preparation

- ✓ Activities performed to “Get Ready”

❖ Mitigation

- ✓ Activities to reduce or eliminate the disruption

❖ Response

- ✓ Activities to occur during and immediately after a disruption

❖ Recovery

- ✓ Activities to return the organization to “normal”



Threats and Hazards

Natural

- > Hurricane
- > Fire
- > Flood
- > Winter Storm
- > Earthquake
- > Pandemic (M1H1, MRSA)
- > Tornado
- > Tropical Storm

Man made / Technical

- > Cyber Attack
- > Bomb Incident
- > Funds Missing
- > Extortion
- > Kidnapping
- > Civil Unrest
- > Arson
- > Deliberate Disruption

Pandemic

- ❑ *Any highly communicable disease that leads to heavy absenteeism (50% +)*
 - Avian Flu
 - MRSA (“super staph”)
 - SARS
 - M1H1

Pandemic Planning

- 1. Have a standard Continuity Plan, which offers a very general framework for any type of disaster**
 - ❖ **Assumes Facility loss**
 - ❖ **Assumes Data/Systems loss**
- 2. Now assume Pandemic**
 - ❖ **test your standard plan assuming you have 50% or less of your staff.**
 - ❖ **Create a secondary plan which references the first, but has different job function triggers**



Threats and Hazards

Fire Planning

- ✓ Use “standard” continuity plan
- ✓ Assume facility and data loss
- ✓ What do you need in first 4 hours
- ✓ What do you need in first 12-24 hours
- ✓ What do you need in first 5 days

Hurricane Planning

- ✓ Evacuate as needed
- ✓ Same as above

The Planning Process

- ✓ **Project Initiation**
- ✓ **Risk Assessment**
- ✓ **Business Impact Analysis**
- ✓ **Emergency Response**
- ✓ **Recovery Strategies**
- ✓ **Plan Development**
- ✓ **Training and Awareness**
- ✓ **Plan Testing / Exercise**
- ✓ **Keep the plan Current**

- ✓ **Senior Management buy-in**
- ✓ **Set specific time frame to develop plan**
- ✓ **Develop a clear mission statement for why to have a plan**



Risk Assessment

- ❑ **Identify Threats and Hazards**
 - ✓ *First 12 hours*
 - ✓ *First 24-48 hours*
 - ✓ *Day 5+*
- ❑ **Assess the probability of high level threats only, then create a general framework that creates flexibility**
- ❑ **Identify how much risk are you willing to take**
- ❑ **Ask yourself how close your business is to the cash register.**



Business Impact Analysis

- Identify key business functions
- Specify the processes that supports these functions
- What is the Infrastructure that support the processes
- Develop a Recovery Time Objective
- Determine weak links and critical paths



Recovery Strategies

- Are your employees safe?
- How do you get back in business?
- Retrieving Back up Data and Systems
- Where do your employees work?
- What is your “New Normal”?
- Recovery Strategy should be based on the Impact Analysis



Emergency Response

- ❑ **Should a disaster occur, what will you do?**
- ❑ **First objectives:**
 - ✓ **Preserve life and personal safety**
 - ✓ **Evacuation or seek shelter on site**
 - ✓ **Communication - Follow call lists**
- ❑ **Initialize the Disaster Response Team**
- ❑ **Response differs from Recovery**

- Write it all down (document, document!!)
- Layout should be easy to use
- Plan should include:
 - ✓ *What happens before an event*
 - ✓ *How an event could be prevented*
 - ✓ *Response to an event*
 - ✓ *Recovery after an event*
- Identify resources / companies who may be needed to support the Plan



Training & Awareness

- Make all stakeholders aware of the Plan**
- Include as part of new staff orientation**
- Frequently refresh staffs knowledge**
- Make participation mandatory**
- Provide for CPR, First Aid and other training**
- Make the Plan a part of the corporate culture**



Essential Plan Testing

- 1. Demonstrates commitment to preparedness**
- 2. Increases Awareness amongst the Management Team**
- 3. Uncovers area in need of improvement**
- 4. Helps development the participants skills**
- 5. Promotes Team Building within the Emergency Response Team**



Current BC and DR Trends defined

- ❑ **Do nothing = out of compliance, lose customers or go out of business**
- ❑ **Offsite data backup**
 - ❖ **Tape**
 - ❖ **Electronic**
- ❑ **“JIT” or Just-in-time hardware solution**
- ❑ **Pre-configured “warm site”**
- ❑ **Hot failover site**
- ❑ **Offsite primary production site**



Current BC and DR Trends

Offsite Data Backup

"JIT" Hardware Solution

Pre-configured "Warm Site"

Offsite Hosting of primary or secondary datacenter

GOAL = DECREASE TIME TO RECOVERY

TIME TO RECOVERY =
Tape: 4-14 days
Electronic: 1-5 days

TIME TO RECOVERY =
?
Too many "what ifs"

TIME TO RECOVERY =
24 to 72 Hours +

TIME TO RECOVERY =
Zero to minutes



Current BC and DR Trends

GOAL = DECREASE RECOVERY TIME = AUTOMATION

Automation allows:

- ❖ Accurate Reporting
- ❖ Security / privacy needs
- ❖ Increased customer access
- ❖ Usage of process experts
- ❖ Ability to offer additional services without additional headcount or minimal investment
- ❖ Outsourcing of backroom operations



Current BC and DR Trends

WHY IS NEED FOR AUTOMATION INCREASING ?

- ❖ Adhere to regulations
- ❖ Usage of Best Business Practices / Efficient Management
- ❖ Legal
- ❖ Offering higher level of service
- ❖ Paper becoming obsolete
- ❖ Digital policy execution
- ❖ Application convergence
- ❖ Greater need for detailed reporting
- ❖ Competition
- ❖ Efficient use of people: outsourcing of backroom ops

“Disaster Recovery and Business continuity is affordable for almost any size organization. This is not just reserved for the large fortune 1000 companies”

Budget:

- ✓ Determine the cost of downtime
- ✓ Define what level of risk you are willing to take
- ✓ Consider staged implementation

Cost:

- ✓ Can implement a plan for as little as a few hundred dollars per month
- ✓ Can begin with offsite electronic backup for as little as \$75.00 per month

A Final Thought

***“Failure to Prepare is
Preparing to Fail”***

Ben Franklin



**We can help you implement your plan in a highly
secure and private environment**



- **Remote Datacenter Co-location/Managed Hosting**
- **Secure Data Storage, Backup & Retrieval**
- **Email Archive and Search capabilities**
- **Continuity Seating & Work Area Recovery**
- **24 x 7 Network Operations Center**
- **Server / Device Monitoring**
- **Complete Managed Services**

On behalf of DataChambers Thank You for your time!

The logo consists of a stylized, three-dimensional circular ring with a metallic texture, positioned behind the company name. The background of the entire slide is a vibrant, abstract blue and cyan pattern with a crystalline or geometric appearance.

DATA CHAMBERS

EJ Schwartz

336.499.7245

eschwartz@datachambers.com

www.datachambers.com