Business Continuity
And Risk Management

Alan L. Sawchak, Senior Consultant
Strohl Systems Group, Inc.
Today’s Topics

• BCP challenges you face
  ▪ How to overcome these challenges
  ▪ Examples of how others are effectively dealing with them

• Highlight a world-class BCP organization
  ▪ Risk Assessment
  ▪ Business Impact Analysis (BIA)
  ▪ Plan Building
  ▪ Testing
  ▪ Maintenance

• Others’ expectations of BCP
Traditional BCP Challenges

- Lack of Interest
- Too much education
- Inefficient spending
- Bad Assumptions
- Lack of Standards
- Decentralized
The Challenges of a Lack of Interest

- Not a documented objective
- Can’t measure the ROI
- Not a concern
- It will never happen
- Too busy to worry about it
- No budget to support it
How to Overcome the Lack of Interest

- Make it a documented objective
- Let them know they are not on an island
- Conduct a BIA for business unit to show them the cost of a disruption
- Conduct a risk assessment for the building they are in
- Work through them, not around them
The Challenges of Too Much Education

- Continuity planner becomes a nag
- Information overload
- BCP information becomes white noise
- Business units rebel
How to Overcome Too Much Education

- Remember: You are the expert
- The organization still has other goals and expectations
- Target the information and the audiences
- Market the concept, don’t oversell it
The Challenges of Inefficient Spending

- Planners ask for overkill
- There is no ROI
- BCP does not generate revenue
- “Can’t we just buy insurance for this?”
How to Overcome Inefficient Spending

- Make BCP “lean and mean”
- Do your homework – explore other options
- Keep BIAs and risk assessments up-to-date
- Show where you have saved money
- Incorporate enterprise-wide BCP
Bad Assumptions

The Challenges of Bad Assumptions

- Business units assume availability of resources or facilities for recovery
- Redundant or inefficient use of resources
- Underutilized resources
- Cost overruns
- Recovery time objectives (RTO) are not realistic and do not incorporate service level agreements (SLA)
- Plan assumptions are out of date
How to Overcome Bad Assumptions

- Review and adjust plan assumptions
- Review SLAs and RTOs
- Test, test, test
- Centralize the planning effort
The Challenges of a Lack of Standards

- Don’t assume standards are followed
- Are your standards really based on best practices?
- Standards are not updated
- Standards are too complicated and therefore not accepted. (If a standard falls in the forest and nobody accepts it, is it still a standard?)
How to Overcome Lack of Standards

- Create standards based on best practices
- Meet with your peers regularly
- Communicate the standards and why everyone needs to follow them
- Periodically review the standards and adjust accordingly
- Measure performance against the standards
The Challenges of Decentralized Planning

- Inflated costs
- Inefficient recovery
- No dependency mapping
- Exasperates previous challenges (Lack of interest, too much education, inefficient spending, bad assumptions, and lack of standards)
How to Overcome Decentralized Planning

- Central repository for data
- Standardize on tools and policies
- Create a steering committee
- Demonstrate value
- Seek a C-level champion
General Risk Assessment Process

Source: Risk Assessment Benchmarks 2000
Natural Risks

- Hurricane
- Earthquake
- Flood
- Mudslides
- Volcano
- Tidal Wave - Tsunami
- Lightning
- Wildfires
- Bomb Threat
- Terrorism
- Extortion
- Vandalism
- Riots/Civil Disturbances
- Burglary
- Data Theft
- Fraud
Technical Risks

- Virus
- Communication Failure
- HVAC Failure
- Power Failure
- Software/System Failure
- Hardware Failure
- Electromagnetic Interference
- Building Infrastructure
• Highways
• Airports
• Train Tracks
• Nuclear Power Plants
• Chemical Laboratory
• Manufacturing Facilities
• Military Bases
Characteristics of Risk

- **Uncertainty**
  What is the probability that risk will occur?

- **Subjective**
  Differing opinions

- **Loss**
  What is the impact of risk if it occurs?
Risk Estimation

- Develop risk table
  - List all risks
  - Categorize each risk
  - Estimate probabilities
  - Analyze impact
  - Sort risks and determine which ones need to be managed

Where will resources be directed?
Risk Estimation

- **Probability**
  What is the *likelihood* that this is going to occur?

- **Severity**
  What is the estimate of the impact/cost?

**Probability x Severity = RISK.**
Evaluate Impact – Sample Rating Scale

- **Low**
  - Low probability with low to medium impact

- **Medium**
  - Medium probability with medium to high impact

- **High**
  - High probability with high impact
The risk assessment should include:

- A prioritization of potential business disruptions based upon severity and likelihood of occurrence.
- An analysis of threats based upon the impact on the institution.
- Human, Natural, and Technical threats.

When assessing the probability of a specific event occurring, companies should consider the geographic location of their facilities and their susceptibility to natural threats, and the proximity to critical infrastructures.

- How often do they occur?
- How much damage can they do?
Recovery processes and procedures should address how the organization would respond if:

- Critical personnel are not available
- Critical facilities or geographic regions are not accessible
- Equipment malfunctions
- Software and data are not accessible or are corrupted
- Vendor assistance or service provider is not available
- Utilities are not available
- Critical documentation and/or records are unavailable

What if?
Risk Mitigation

- Eliminate threats if possible – this can have the biggest impact on insurance costs
- Identify effective controls to reduce risks and insurance costs
- Evaluate risk, life safety, cost etc.
- Implement protective/preventative measures
  - Generators/Fuel
  - Fire Suppression Systems
  - Emergency Water Supply
  - Fire and Security Alarm Systems
  - Proper Chemical Storage
  - Controlled Building Access – ID Badges
  - Building Supports
  - Data and Information Security Controls
  - Back Up Procedures
Risk Management involves:

- Analysis of threats most likely to occur.
- Identifying threats that are the most destructive.
- Acknowledgement of unanticipated threat scenarios and changing internal conditions.
- Minimizing service disruptions and financial loss.
- Having a contingency plan for mitigating risks.
DMSP F15
15 August 2003
0114Z
~7 hrs after Blackout

Brightness in Boston is unchanged
Brightness in Long Island is MUCH reduced

Toronto
Ottawa
Montreal

Detroit
Cleveland
Columbus

Buffalo
Albany
## Risk Assessment

<table>
<thead>
<tr>
<th>Event</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Volcano</td>
<td>0</td>
</tr>
<tr>
<td>Hurricane</td>
<td>+10</td>
</tr>
<tr>
<td>Tornado</td>
<td>+10</td>
</tr>
<tr>
<td>Earthquake</td>
<td>+20</td>
</tr>
<tr>
<td>Flood Plain</td>
<td>0</td>
</tr>
<tr>
<td>Above 100 Year Line</td>
<td>0</td>
</tr>
<tr>
<td>River/Coastline/Dam</td>
<td>+6</td>
</tr>
</tbody>
</table>
Risk Assessment

Nuclear Plant ✓ +4
Research Lab ✓ +3
Airport ✓ +2
Military Base ✓ +2
Landfill ✓ +2
Chemical Factory ✗ 0
Others ✗ 0

Risks = +59
World-class BCP Program

Risk Mitigation

- Earthquake Proof: 🚗 -3
- Satellite/ Microwave Communications: 🎯 -2
- Telecommunications Routing Diversity: 🎯 -3
- Independent Water Supply: 🎯 -3
- Redundant Chillers: 🎯 -3

Mitigation = -11
Risk Rating

Risks: +59
Mitigation: -11

Overall Risk Rating = 48

Index
>50 – High Risk
28-49 – Medium Risk
13-27 – Low Risk
< 13 – Good BCP Potential

Each risk category is considered (+/- impact rating).

The risk rating for recovery sites should be less than 27
Changes in Risk Assessments?

- **Old Assumptions** – in the past a business could assume that if the main office was in NY, and the backup was in Chicago, the staff would just fly to the backup location in the event of an unplanned disruption.

- **New Perspectives** – No one ever planned for all airlines being grounded – but it happened.
Risks Are Always Changing

- Threat Assessment – imagine the unimaginable
- New Biological and Chemical Threats
- Virus and Disease
- Internal Requirements - enterprise-wide planning
- Responsibilities of Board of Directors and Senior Management have increased
- Recovery Time Objectives – becoming shorter and shorter
- Interdependency
- Technology dependence outside the organization
Business Impact Analysis

• A ROI is an analysis of cost impacts of a decision – SO IS A BIA.

• Discovers vulnerabilities – operational and financial

• Sets strategies for recovery

• Foundation of the plan
## Business Impact Analysis

Corporate Category: Global Healthcare

### BIA IMPACT DATA

<table>
<thead>
<tr>
<th>Impact Category</th>
<th>Severity</th>
<th>Volume</th>
<th>Volume Type</th>
<th>Can Stand Down</th>
<th>Work from Home</th>
<th>Equipped from Home</th>
<th>Recovery Time Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Service Impact</td>
<td>HIGH</td>
<td></td>
<td></td>
<td></td>
<td>YES</td>
<td>NO</td>
<td>DAY 2</td>
</tr>
<tr>
<td>Share Confidence</td>
<td>HIGH</td>
<td></td>
<td></td>
<td></td>
<td>YES</td>
<td>NO</td>
<td>DAY 2</td>
</tr>
<tr>
<td>Industry Image</td>
<td>HIGH</td>
<td></td>
<td></td>
<td></td>
<td>YES</td>
<td>NO</td>
<td>DAY 2</td>
</tr>
<tr>
<td>Competitive Advantage</td>
<td>MEDIUM</td>
<td></td>
<td></td>
<td></td>
<td>YES</td>
<td>NO</td>
<td>DAY 2</td>
</tr>
<tr>
<td>Financial Impact</td>
<td>HIGH</td>
<td></td>
<td></td>
<td></td>
<td>YES</td>
<td>NO</td>
<td>DAY 2</td>
</tr>
<tr>
<td>Service Level Agreements</td>
<td>HIGH</td>
<td></td>
<td></td>
<td></td>
<td>YES</td>
<td>NO</td>
<td>DAY 2</td>
</tr>
<tr>
<td>Other – Please Specify</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>YES</td>
<td>NO</td>
<td>DAY 2</td>
</tr>
<tr>
<td>Increase in Liability Impact</td>
<td>HIGH</td>
<td></td>
<td></td>
<td></td>
<td>YES</td>
<td>NO</td>
<td>DAY 2</td>
</tr>
<tr>
<td>Financial Reporting Impact</td>
<td>LOW</td>
<td></td>
<td></td>
<td></td>
<td>YES</td>
<td>NO</td>
<td>DAY 2</td>
</tr>
<tr>
<td>Operational/Workflow Impact</td>
<td>LOW</td>
<td></td>
<td></td>
<td></td>
<td>YES</td>
<td>NO</td>
<td>DAY 2</td>
</tr>
<tr>
<td>Employee Morale Impact</td>
<td>LOW</td>
<td></td>
<td></td>
<td></td>
<td>YES</td>
<td>NO</td>
<td>DAY 2</td>
</tr>
<tr>
<td>Other Impact Rating</td>
<td>MEDIUM</td>
<td></td>
<td></td>
<td></td>
<td>YES</td>
<td>NO</td>
<td>DAY 2</td>
</tr>
<tr>
<td>Impact Amount (US$)</td>
<td>$1M</td>
<td></td>
<td></td>
<td></td>
<td>YES</td>
<td>NO</td>
<td>DAY 2</td>
</tr>
<tr>
<td>Load Balance at the Other Facilities</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>YES</td>
<td>NO</td>
<td>DAY 2</td>
</tr>
</tbody>
</table>

### RECOVERY STRATEGY

Load Balance at the Other Facilities

### YTD IMPACT HISTORY

<table>
<thead>
<tr>
<th>Impact Type</th>
<th># of Occurrences</th>
<th>Longest Duration</th>
<th>Impact Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Loss</td>
<td>YES</td>
<td>3</td>
<td>DAY 1</td>
</tr>
<tr>
<td>Fire</td>
<td>NO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Loss of Voice</td>
<td>YES</td>
<td>1</td>
<td>DAY 1</td>
</tr>
<tr>
<td>Loss of LAN Access</td>
<td>YES</td>
<td>5</td>
<td>DAY 1</td>
</tr>
<tr>
<td>Severe Weather</td>
<td>YES</td>
<td>1</td>
<td>DAY 1</td>
</tr>
</tbody>
</table>
Plan Building

Internal Site A - Maximum:
• 100 Seats with IBM PL300 Workstations
• 50 Seats with ACD

Total Plan Requirements:
• 250 Seats with IBM PL300 Workstations
• 100 Seats with ACD
Plan Building

Hotsite Vendor - Maximum:
- 200 Seats with IBM PL300 Workstations
- 40 Seats with ACD

Plan Requirements:
- 40 Seats with IBM PL300 Workstations
- 10 Seats with ACD

DR Assets Available @ Vendor:
- 160 Seats with IBM PL300 Workstations
- 30 Seats with ACD
## Plan Building

Corporate Category: Global Healthcare

### Site A: Training Room

<table>
<thead>
<tr>
<th>Required Seats</th>
<th>Available Seats</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LAN</strong></td>
<td><strong>Voice</strong></td>
</tr>
<tr>
<td>Finance Recovery Plan</td>
<td>45</td>
</tr>
<tr>
<td>Trading Recovery Plan</td>
<td>10</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>55</td>
</tr>
</tbody>
</table>

**WARNING: Not enough seats available!**

### Site B: Hotsite Vendor – Houston, TX

<table>
<thead>
<tr>
<th>Required Seats</th>
<th>Available Seats</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LAN</strong></td>
<td><strong>Voice</strong></td>
</tr>
<tr>
<td>Call Center</td>
<td>15</td>
</tr>
<tr>
<td>Human Resources</td>
<td>5</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>20</td>
</tr>
</tbody>
</table>

**Plenty of seats available**
Plan Testing

**IT RTA (exercised result):**
Can deliver 100 clients:
- Bloomberg (< 4 hours)
- PeopleSoft (24 hours)
- Notes (3 days)

**Leanest RTO @ Site:**
100 clients need:
- Bloomberg <4 hours
- PeopleSoft <1 hour
- Notes <1 hour
## BCP PLAN A (PROCESS MISSION CRITICAL)

<table>
<thead>
<tr>
<th>Client Access for Seats 1A</th>
<th>0-4</th>
<th>4-8</th>
<th>8-24</th>
<th>2 DAYS</th>
<th>3 DAYS</th>
<th>4 DAYS</th>
<th>5 DAYS</th>
<th>2 WEEKS</th>
<th>4 WEEKS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intranet</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PeopleSoft</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Notes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MS Office</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bloomberg Market Feed</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**$12M IMPACT**

## BCP PLAN B (PROCESS MISSION CRITICAL)

<table>
<thead>
<tr>
<th>Client Access for Trading Seats</th>
<th>0-4</th>
<th>4-8</th>
<th>8-24</th>
<th>2 DAYS</th>
<th>3 DAYS</th>
<th>4 DAYS</th>
<th>5 DAYS</th>
<th>2 WEEKS</th>
<th>4 WEEKS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notes</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MS Office</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bloomberg Market Feed</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PeopleSoft</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intranet</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**$400,000 IMPACT**

## BCP PLAN C (PROCESS DEPENDENCY CRITICAL)

<table>
<thead>
<tr>
<th>Client Access for Trading Seats</th>
<th>0-4</th>
<th>4-8</th>
<th>8-24</th>
<th>2 DAYS</th>
<th>3 DAYS</th>
<th>4 DAYS</th>
<th>5 DAYS</th>
<th>2 WEEKS</th>
<th>4 WEEKS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proprietary Trading Solution</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bond Data System</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intranet</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Derivatives Trading Tool</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Investment Research Tool</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**RTO = X**  **RTA = X**
Plan Maintenance

- Plans are reviewed periodically
- Current data is imported weekly
- Tests are scheduled
- Plan is constantly reviewed against test results and new techniques, procedures, and standards
- RTOs are reviewed against SLAs
- Vendors are audited
Hallmarks of a World-class BCP Program

- Centralized
- C-level champion
- Steering committee
- Buy-in at all levels
- Generally accepted standards
- Enterprise wide
- Constant review and testing
- Cost effective
Which department in your organization is ultimately responsible for business continuity planning?
BCP Expectations of Others

What does your plan cover?

Percent of Responses

- All Business Units
- Key Internal Functions
- Only IT Functions

2002
2003

0 10 20 30 40 50 60

Percent of Responses
## Business Continuity Maturity Model

**Virtual Corporation**

<table>
<thead>
<tr>
<th>Competency Maturity Level</th>
<th>Program Basics</th>
<th>Program Development</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Sr. Mngt. Commitment</td>
<td>Professional Support</td>
</tr>
<tr>
<td>Level 1</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Self-Government</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Level 2</td>
<td>Marginal</td>
<td>Partial</td>
</tr>
<tr>
<td>Supported Self-Government</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Level 3</td>
<td>Partial</td>
<td>Yes</td>
</tr>
<tr>
<td>Centrally Governed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Level 4</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Enterprise Awakening</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Level 5</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Planned Growth</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Level 6</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Synergistic</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note:**

- **Synergistic** indicates a fully integrated and aligned approach across all business units.
- **Level 6** represents the highest level of maturity, where all business units are fully aligned and integrated in their business continuity planning.

---

**STROHL SYSTEMS**

+1-610-768-4120  Toll free: 800-634-2016  |  info@strohlsystems.com  |  www.strohlsystems.com
How Mature is your Business Continuity Program?

- **Level 1 - Self-Governed** - Business continuity management has not yet been recognized as strategically important by senior management.

- **Level 2 - Supported Self-Governed** - At least one business unit or corporate function has recognized the strategic importance of business continuity and has begun efforts to increase executive and enterprise-wide awareness.

- **Level 3 - Centrally-Governed** - Participating business units and departments have instituted a rudimentary governance program, mandating at least limited compliance to standardized BCM policy, practices and processes to which they have commonly agreed.
How Mature is your Business Continuity Program?

- **Level 4 - Enterprise Awakening** - All critical business functions have been identified and continuity plans for their protection have been developed across the enterprise.

- **Level 5 - Planned Growth** - Business continuity plans and tests incorporate multi-departmental considerations of critical enterprise business processes.

- **Level 6 - Synergistic** - All business units have a measurably high degree of business continuity planning competency. Complex business protection strategies are formulated and tested successfully.
BCP is another form of insurance

- Insurance only mitigates risk
- Business disruption insurance does not cover lost customers or damage to a reputation
- BCP and insurance are complementary
BCP is a NOT Project

- BCP is a Program
- Y2K contingency plans that were a project will not work now
- Must be continually evaluated and adjusted
- Needs annual budget
Regulations and SLAs will not change

• Regulations are effecting every industry
• With each new major event, regulations are sure to follow
• Current regulations are being modified
• Every time there is a new customer, there are new obligations
• New technology requires reduced SLAs
There is a way to calculate ROI for BCP

- There is no way to calculate ROI for an unforeseen event that you hope will not happen
- The closest way to prove value is to conduct a BIA
- Use demonstrated value to prove effectiveness
- Make BCP “lean and mean” – be cost conscious
BCP Expectations of Others

Have you ever had to activate your plan for any reason?

Percent of Responses

Yes | No | Don't Have Plan

Percent of Responses

0 10 20 30 40 50 60

Yes | No | Don't Have Plan
Have you ever experienced an interruption that caused you to activate any documented recovery steps?

Source: Continuity Insights/KPMG Business Continuity Benchmarking Survey
Of the 49 percent who did not have to activate all or part of their plan in the last year, they either:

- Lied on the survey
- Have no plan
- Have thought of every possible contingency and mitigated them completely out of existence
- Have been extremely lucky
"We have no clue. Our computer is giving us fits too. We don't even know the status of some of the stuff around us…"

(operator at Akron-based FirstEnergy said in an excerpt of a 650-page transcript released by the House Energy panel)
“The nicest thing about not planning is that failure comes as a complete surprise and is not preceded by a period of worry and depression.”

~John Preston
Boston College
Business Continuity
And Risk Management

Alan L. Sawchak, Senior Consultant
Strohl Systems Group, Inc.