

Using Facilitated Methods to Perform Business Impact Analysis

Brian Zawada (CISA, CBCP)
Product Leader, Business Continuity Management Services

Presentation Overview

- What is Business Continuity Management?
- Demo – “Resolver Ballot”
- Why Plan for Business Interruptions?
- The Business Impact Analysis (BIA) & Common Criticisms
- Methodologies and Approaches to Conduct the BIA
- “Tools” Available to Execute a BIA
- Presenting the Results of the BIA
- Demo – Process Modeling and Simulation Software
- Lessons Learned from 9/11
- Questions and Discussion

Business Continuity Management (BCM) Defined

Business Continuity Management

...the development of *strategies, plans* and *actions* which provide protection or alternative modes of operation for those activities or business processes which, if they were to be interrupted, might otherwise bring about a seriously damaging or potentially fatal loss to the enterprise.

BCM = Crisis Management + Business Resumption Planning + IT Disaster Recovery Planning

Components of a BCM Process

Business Continuity Management

- Process Governance
- Tested, Documented Procedures
- Crisis Organizational Structure
- Emergency Operations Center
- Alternate Processing Facility
- Crisis Communications Process
- Trained Personnel
- Pre-positioned Resources
- Identified Vital Records, Information & Data
- Training and Awareness Program
- Plan Testing & Exercise Program
- Plan Maintenance Process
- Process Owner

Demo – “Resolver Ballot”

BCM Key Success Factor –
Establish Executive Management Buy-in

Why Plan for Business Interruption?

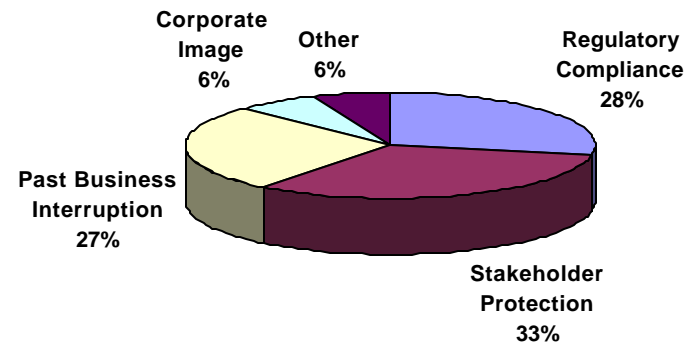
Business Continuity Management

- Customer Service Level Agreements & Demands
- The Odds of an Interruption
- The Consequences of an Interruption
- The “Lean” Organization that Lacks Redundancy and Excess Capacity
- Regulatory Requirements and Associated Fines/Penalties

BCM-related Statistics

Business Continuity Management

Primary Reasons Organizations Have a BCP (2002)



CPM July/August 2002

Methodologies and Approaches to Conducting the BIA

Business Impact Analysis

- BIA Defined
 - The careful study of individual business processes and support functions, as well as the system of business processes in its entirety, to better understand objectives regarding continuity of operations
- The “BCP Blue Print”
- The Business Case for BCM
- The relationship between the BIA and the Risk Assessment
- Change in Scope - The Extended Enterprise
- Objectives
 - Quantify the loss potential
 - Qualify other types of loss
 - Establish RTO
 - Establish RPO
 - New Term – RCO?
- Common Criticisms...

Common Criticisms of the BIA

Business Impact Analysis

- The results are too high level
- Those numbers can't be right
- You assumed the worst-case scenario
- Weak approach
- "Yeah, but it depends..."
- That part of the business isn't that critical - they're just trying to justify their jobs!
- You collected the wrong information from the wrong person

Methodology and Approach to Conducting the BIA

Business Impact Analysis

- Work through a Steering Committee
- Identify what the deliverables should look like and the desired content
- Develop an initial scope
- Identify process-level subject matter experts
- Develop data gathering plan
- Summarize findings
- Conduct analysis and develop conclusions
- Validate findings with subject matter experts
- Present validated findings to executive management for buy-in
- Transition to strategy development

BIA Data Sources

Business Impact Analysis

- What type of data sources should I use?
 - Use existing process flows, policies and procedures
 - Loss prevention reports
 - IT system or application logs
 - Audit reports
 - Financial reports
 - Departmental budgets
 - Production schedules
 - The results from process modeling
 - How does your organization forecast business and measure results?

BIA Data Requirements

Business Impact Analysis

- What type of data should I be looking for?
 - Customers (and SLAs)
 - Personnel (to include cost of employment and schedules)
 - Resources
 - Equipment
 - Production schedules and timing (cycle times, peaks, start/stop times, variance)
 - IT requirements
 - Communications needs
 - Vital records and data needs
 - Dependencies and interdependencies
 - Throughput
 - Risk perception
 - Regulatory requirements
 - Existing data and records backup/management process
 - Existing manual workarounds

BCM Regulatory Requirements

Business
Impact
Analysis

- NFPA 1600
- HIPAA
- GLBA
- FFIEC
- OSHA
- FCPA
- SEC
- ISO 9000 & 14000
- QS 9000
- State Insurance Departments
- Critical Infrastructure Protection
 - Security Standards for Electric Market Participants
 - Sound Practices to Strengthen the Resilience of the US Financial System

BIA Data Collection Mechanisms

Business Impact Analysis

- What are the best ways to collect the best data?
 - Questionnaires
 - Facilitated Sessions
 - Data intensive methodologies like Six Sigma
 - Research third-party data sources

www.fema.gov

www4.ncdc.noaa.gov

www.nhc.noaa.gov

whirlwind100.nssl.noaa.gov

www.eei.org

The Facilitated Session

Business Impact Analysis

- Plan to Conduct the Facilitated Session
 - Customers
 - Products and Services
 - Vendors and Suppliers
 - Other Process Inputs
 - Technology Usage
 - Process Level Steps
 - Revenue or Production Numbers
 - Cycle Time
 - Personnel Costs
 - Facility Costs
 - Fixed Equipment Costs
 - Brainstorming Risks

Provide discussion topics in advance so participants are prepared

Potential Impacts of an Interruption...

Business Impact Analysis

- What conclusions should I reach, based on my analysis?
 - Work Stoppage
 - Opportunity Costs
 - Idle Workforce and Resources
 - Regulatory Noncompliance
 - Financial Loss
 - Loss of Investor Confidence
 - Reputation Impairment
 - EHS Impairment (OSHA)
 - Loss of Market Share
 - Lost Sales
 - Cash Flow Interruption
 - Financial Control/Reporting
 - Customer Service
 - Vendor Relations
 - Employee Morale/Retention
 - Market Reaction
 - Contractual Default
 - Lost Discounts

Presenting the Results of the BIA

Business Impact Analysis

- What are the best ways to summarize the data I've collected and the conclusions I reached?
 - It really depends on the culture of the organization and its management
 - “A picture is worth a thousand words”

Sample BIA Deliverables

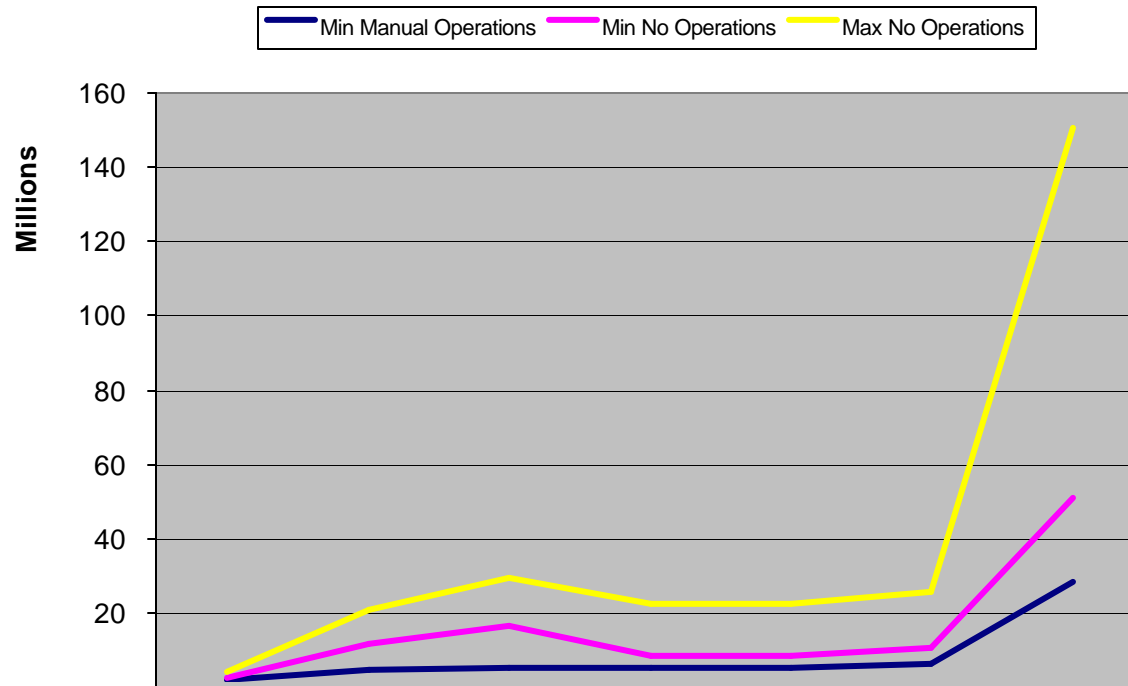
System/ Application/ Connectivity	Cust. Service	E-Commerce	Shipping	Inventory	Corporate Payroll	Business Process	Recovery Time Objective
Corporate Payroll	48	n/a	72	n/a	12	Payroll	12
E-Commerce System	0	0	0	n/a	n/a	Cust. Service E-Commerce Shipping	0
EDI	24	n/a	48	24	n/a	Cust. Service Inventory	24
ERP	12	24	0	<12	12	Shipping	0
Fax Router	72	n/a	n/a	n/a	n/a	Cust. Service	72
Financial System	>72	n/a	n/a	n/a	n/a	Cust. Service	>72
Forecasting/Budgeting	n/a	n/a	n/a	48	n/a	Inventory	48
FTP	n/a	n/a	n/a	n/a	12	Payroll	12
Intranet	>72	n/a	n/a	n/a	n/a	Cust. Service	>72
Inventory System	0	0	0	n/a	n/a	Cust. Service E-Commerce Inventory	0
ISDN	n/a	n/a	n/a	n/a	24	Payroll	24
Lotus Notes	72	n/a	n/a	n/a	72	Cust. Service Payroll	72
Network Server	n/a	n/a	72	n/a	72	Shipping Payroll	72
PBX System	0	n/a	n/a	n/a	n/a	Cust. Service	0
Sales Order System	0	n/a	n/a	0	n/a	Cust. Service Inventory	0
Scanners	n/a	n/a	48	n/a	n/a	Shipping	48
VAN	24	n/a	n/a	n/a	n/a	Cust. Service	24
WAN	n/a	0	12	12	n/a	E-Commerce	0

Application	Recovery Time Objective	Business Process(es) within RTO Timeframe	Recovery Point Objective	Business Process(es) within RPO Timeframe	Lowest Recovery Time Objective
ERP	0-24 hours	Shipping Customer Service	0-24 hours	Customer Service Shipping Inventory	Customer Service
E-Commerce	0-24 hours	Customer Service Shipping E-Commerce	0-24 hours	Shipping	Customer Service
Inventory	0-24 hours	E-Commerce	0-24 hours	Customer Service Shipping	Customer Service
Sales Order System	0-24 hours	Inventory Customer Service	25-72 hours	Inventory Customer Service	Customer Service
Corporate Payroll	0-24 hours	Payroll Customer Service	0-24 hours	Payroll	Payroll
Forecasting/ Budgeting	25-72 hours	Inventory	0-24 hours	Inventory	Inventory
Financial	1-3 weeks	Customer Service	1-3 weeks	Customer Service	Customer Service

Recovery Timeframe Legend	
0-24 hours	
25-72 hours	
>72 hours	

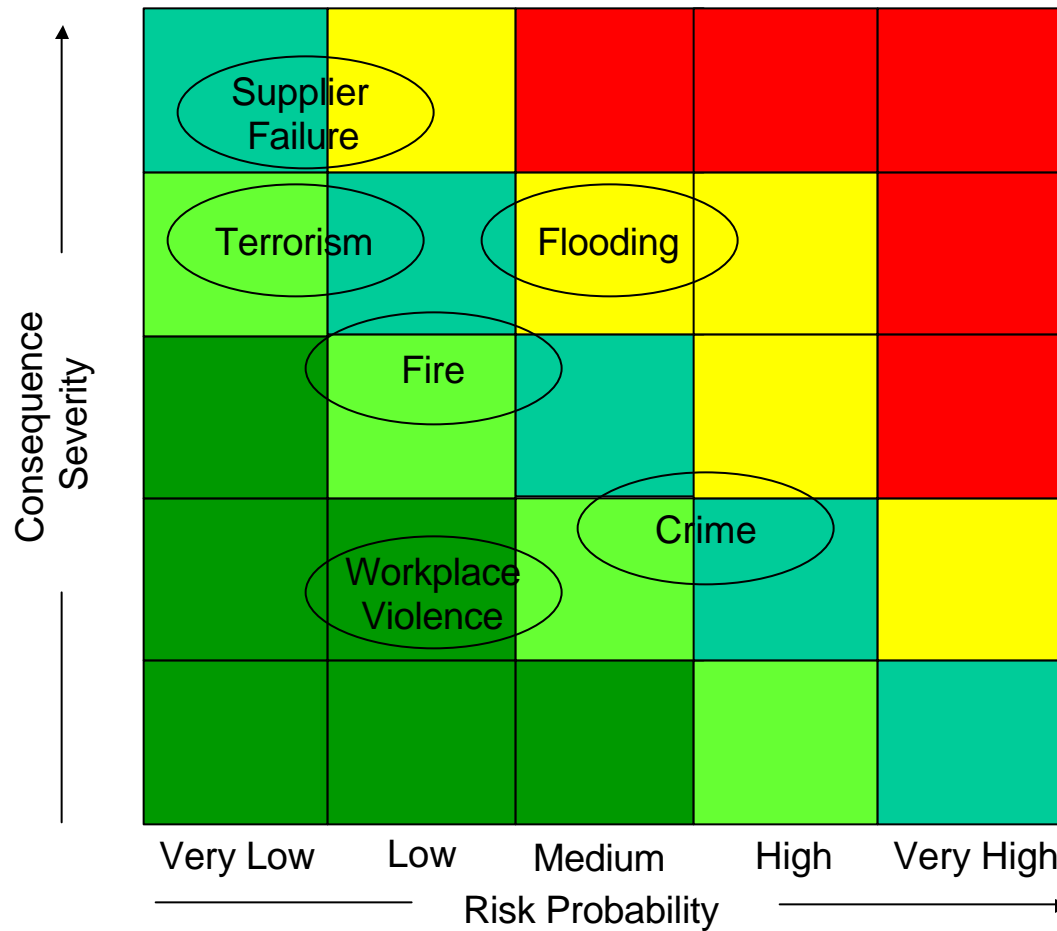
Sample BIA Deliverables

Revenue Lost and Add'l Costs



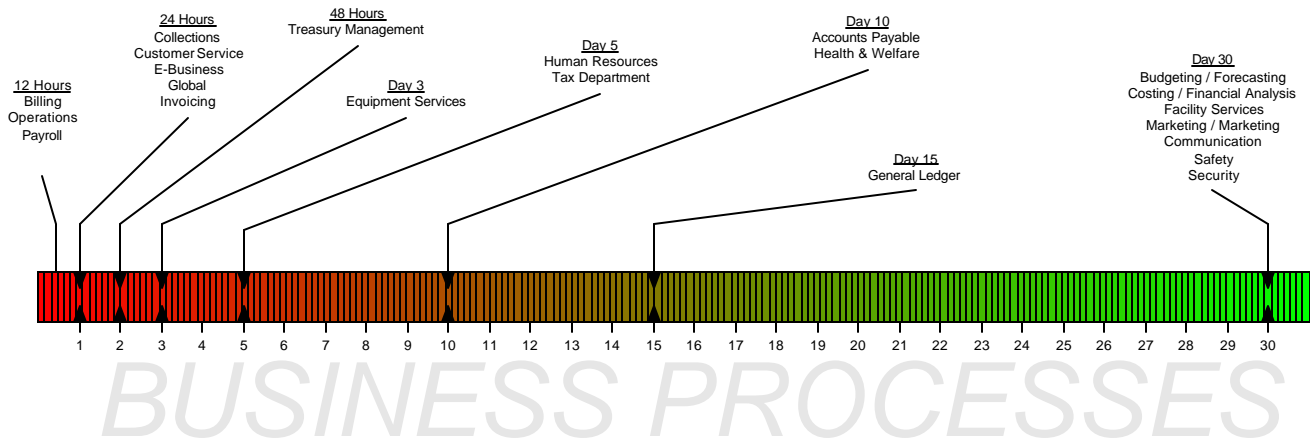
	0 - 12 hours	12-24 hours	Day 2	Day 3	Day 4	Day 5	Week 2
Max No Operations	1,300,387	8,765,231	13,008,765	14,098,768	14,098,768	15,197,273	99,653,194
Min No Operations	879,000	7,200,000	11,345,998	3,200,857	3,200,857	4,509,736	23,000,657
Min Manual Operations	274,000	3,161,000	3,639,000	3,647,000	3,677,000	4,753,800	26,694,800

Sample BIA Deliverables



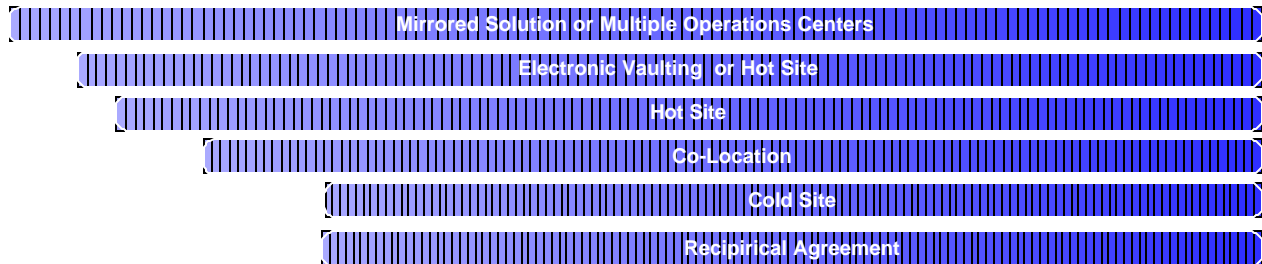
Prioritize Risks
Likelihood x Severity x Detectability

Sample BIA Deliverables

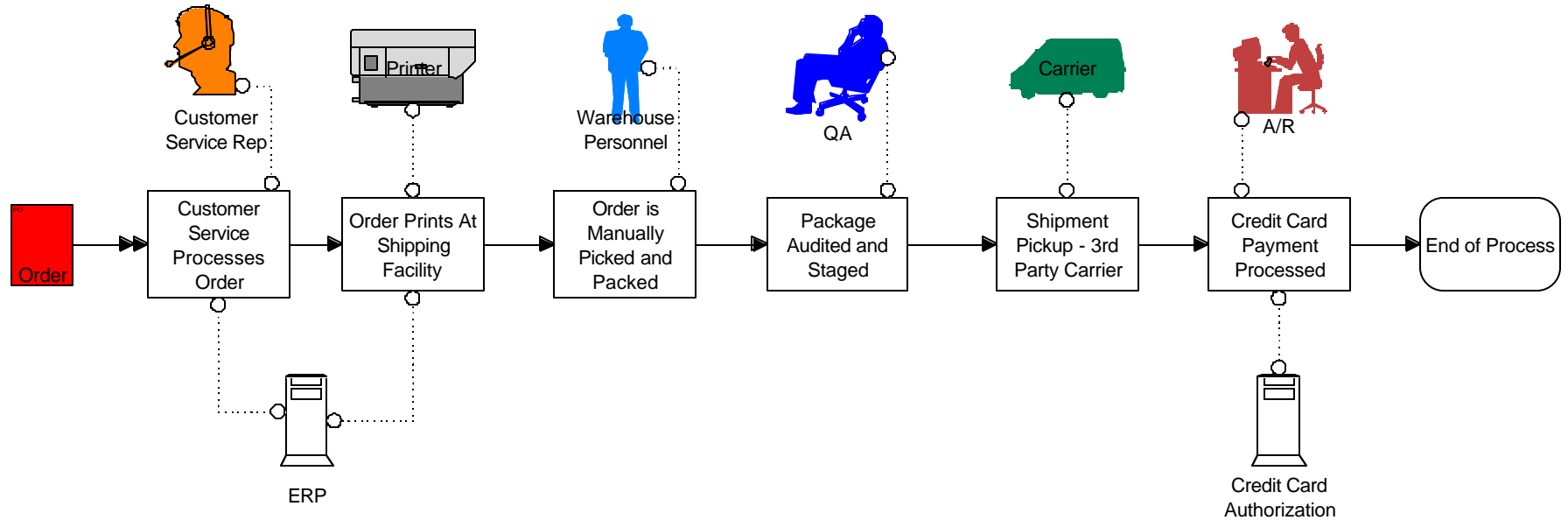


BUSINESS PROCESSES

Recovery Alternatives



Sample BIA Deliverables



Demo – Process Modeling

One way we have found to conduct a “rigorous” BIA is to use process modeling software.

Demo – “Resolver Ballot”

BCM Key Success Factor –
Establish Executive Management Buy-in

Presentation Summary

Business Continuity Management

- Clarified what business continuity means, and what the BIA is meant to address
- Approaches to meeting a variety of BIA objectives
- Scope the BIA process early with the steering committee (discuss deliverables then)
- The importance of a data collection plan that utilizes objective data sources
- Be creative – a variety of in-house and third-party tools (not necessarily meant for BIAs) may exist
- Presentation of the BIA results may be just as important as the results themselves
- Learn from recent events

Lessons Learned from 9/11/01

Lessons Learned

“It was clear that decisions made by key institutions regarding their individual level of preparedness for disasters and other crises significantly affected others...”

- Identify critical activities
- Determine appropriate recovery objectives
- Maintain sufficient out-of-region resources to meet objectives
- Routinely use of test recovery arrangements
- Cross-train staff at remote sites
- Ensure backup sites have access to current data
- Develop flexible plans
- Require a certain percentage of employees to telecommute each day
- Y2K Plan Deficiencies – backup routines, facilities and contact information were no longer up-to-date
- Business continuity planning has not taken into account the potential for wide-area disasters and for major loss or inaccessibility of critical staff

Source: The Securities and Exchange Commission

Lessons Learned from 9/11/01 (cont.)

Lessons Learned

“In fact, the most oft-cited lesson learned is the importance of people.”

- Many plans focused on single facility disasters
- Some firms arranged to have their backup sites in nearby buildings
- Many firms thought they achieved communications redundancies through multiple vendors
- Out-of-date software, reduced (insufficient) systems capacity and inadequate telecommunications were discovered after plan activation
- Some firms had to devote significant amounts of time to records reconstruction because off-site rotations occurred once a week
- Some disaster recovery vendors found they could not house all of their clients
- Assumptions regarding the length of time a primary site may be incapacitated were flawed
- Organizations with tested BCPs were able to locate and communicate better with internal staff

Source: The Securities and Exchange Commission

Lessons Learned from 9/11/01 (cont.)

Lessons Learned

- Personnel trauma and stress was significant, and increased each day
- Companies did not update their capacity requirements as their environments grew
- Many recovering organizations experienced significant network issues
- Companies seriously underestimated how long it would take to recover – some attributed this to a loss of staff
- There should have been more testing with end users
- Few organizations had work station recovery plans for their end users
- Data synchronization issues surfaced because organizations did not test interfacing systems
- Some companies suffered significant vital records problems because of issues with off-site storage and data backup
- Companies are not prepared to lose recovery team personnel and backups should be trained

Source: The Gartner Group



Discussion and Questions



Contact Information

Brian J. Zawada (CBCP, CISA)
Senior Manager

brian.zawada@protiviti.com
216.479.6872 (office)
330.321.8650 (mobile)

Presentation Abstract

The attacks on New York and Washington in September, and the bio-terrorism events of October, led most organizations to revisit their business continuity management processes. Despite this renewed interest, to include customer mandates for continuity of operations processes, funding for business continuity wasn't budgeted, and budget variances were minimal. Certainly the economy has been a factor, but internal business continuity professionals have also indicated they are having a hard time making the business case for increased BCP investment. Taken one step further, our clients have pointed to the Business Impact Analysis as the key issue. Executives are finding that the BIA results are too high-level, incomplete or aren't rooted in business reality.

Our presentation will focus on ways to bridge the gap between the business continuity professional and the executive-level decision-maker using a rigorous, business-oriented BIA methodology. We will highlight strategies and tools that can assist the planner, as well an outline of the information that should be compiled and presented to the C-level executive.