Business Continuity: We’ve Identified the Risks, Now What?

Customer Supplier 2009 Symposium
Betty A. Kildow, CBCP, FBCI
Emergency Management Consultant
Agenda

- Business Continuity: A Shared Understanding
- Best Practices and Challenges
- A Holistic, Integrated Approach
- Standards, Regulations, and Requirements
Evolution of Business Continuity

- Emergency preparedness & response
- 1950–60’s: backup copies of data
- Early–1970’s: Recognized the need to restore technology
- Late–1970’s: Term Disaster Recovery first used
- Early– to mid–1990’s: Business Recovery was added to disaster planning process
- Late 1990’s: Business Continuity became the more widely–used term
**Business Continuity Is**

- Timely and orderly continuation of or rapid restoration of delivery of the organization’s service or product following a disaster.
- Strategies and plans developed from the perspective of keeping the most critical functions running while normal operations are restored.
Business Continuity Is Not

- Business as usual
  - Think in terms of *survival* not *business as usual*
- Recovery of only the Data Center
  - Disaster Recovery: Restoration of technology to provide IT, telecommunications, and related technology needed to support business continuity objectives
Purpose of Business Continuity

- Manage the risks to enable delivery of services or products, ensuring that operations can continue in the event of a disruption.
- Provide strategic framework for improving an organization’s resilience to interruption.
- Facilitate the recovery of key business systems and processes within agreed timeframes, while maintaining critical functions and delivery of product/service.
Managing the Risks

- CEO: Reputational risks
- CFO: Financial risks
- CIO: IT infrastructure risks
- COO: Operational risks
- CSO: Risks from internal or external attacks

Business continuity is a team approach to address the above...and more...through a strategic *enterprise-wide* approach.
Business Continuity Drivers

- Regulation / legislation
- Government
- Auditors: internal/external
- Insurers
- Customers
- Protection of brand, market share, reputation
- Corporate policy
- Other stakeholders
Object of the Game

To never have to explain to anyone why you could not fulfill any aspect of your business.
The need for a comprehensive program to prepare for and respond to disasters is greater than ever. Everyone has responsibility for safety, security, and business continuity.
During lunch today you receive a call from a colleague from work.
This morning there was a fire in your building that caused significant smoke and water damage to the structure and its contents.
Was your organization prepared?
Are you prepared?
What Do You Do?

- Do you know what is expected of you?
- Do you know how you will be advised when and where to report and by whom?
- Does your organization have an alternate work site?
  - Where is it?
- Do you have a list of emergency contact numbers with you?
  - Is it current?
Goal: Protect the organization, its people, physical assets, and operational capability

A management issue

Impacts the entire organization

Needs to include the entire organization

More than a “Plan”

- Mitigation
- Preparedness
- Response
- Recovery
Development Process

- Identify risks; mitigate to extent possible/practical
- Identify mission critical business functions, and their related time requirements and dependencies (BIA)
- Develop Business Continuity strategies
- Develop plan documents to support strategies
- Implement and test the plans

An Ongoing Process
Basic Disaster Categories

- Natural
- Technological
- Incited (Human-Caused)

Risks may be internal or external, direct or indirect...or inherited.
Business Impact Analysis

- The foundation of the business continuity planning process
- Identifies and prioritizes (time-)critical business functions throughout the organization
- Considers the potential losses if the function were to be halted:
  - Financial losses
  - Lost customers
  - Reputational damage
  - Regulatory effects
- Identifies the maximum acceptable downtime for each
- Identifies minimum needed resources for each
Who Is Responsible?

- Each employee
- Each department
- Business Continuity Planning Group
- Business Continuity Manager/Coordinator
- Executive management
- Board of Directors
Growing Awareness

- Supply chain is susceptible to potentially crippling disaster–caused disruptions
- Must be fully considered and integrated in a comprehensive business continuity program
- Supply chain must function in the face of our complex and at times dangerous world
Supply Chain Challenges

- Complex procurement processes
- Just-in-time inventories
- Ongoing pursuit of efficiency
- Decreased slack in the supply chain
- Smaller lead-time margins
- Increased number of new products
- Continuing growth of the global economy
- Greater reliance on technology
- Extended hours of operation 24/7/365
- Stringent service level agreements
- More outsourcing
- AND…
Growing Importance of External Interdependencies

- Relationships that encompass organizations your company:
  - Sells to
  - Buys from
  - Exchanges data with
  - Relies upon to conduct business
  - Interacts with in some electronic manner
Managing Supplier Risks

- **Business Continuity Manager:**
  - Identify all critical suppliers
  - Understand the impact the loss of a supplier on operations
  - Fully assess all potential risks which could impact identified suppliers
  - Include the supply chain in the business continuity program

- **Purchasing/Procurement:**
  - Make risk aware decisions
  - Develop purchasing strategies that will mitigate supplier risk
  - Take the supplier fully into account, not only the product and the price
  - Monitor suppliers for “red flags”
Developing Supply Chain Continuity

- Map your supply chain
- Identify most critical:
  - Most critical suppliers
  - Single points of failure
  - Internal dependencies
  - IT and other requirements
- Develop strategies
Retail and wholesale

Corporate Headquarters Office

Management, planning, direction; point of sale/ inventory control; process money from sales

Merchandise shipping and tracking

Banks, credit card companies

Reports to Board, stockholders, regulatory/ governmental agencies, etc.
Customer–Supplier Partnering

- An on-going, mutually beneficial relationship between a customer and a supplier.
- A form of collaborative working between customers and suppliers
- Enables working together more effectively when disasters occur
Tough Economic Times

- Those with no Business Continuity Program may:
  - Postpone or eliminate business continuity planning from their budget

- Those with an existing program may:
  - Put program in a holding pattern
  - Eliminate updates, cancel testing
  - Downsize those with key business continuity roles/responsibilities

BUSINESS CONTINUITY EXPO
It is with regret that due to the current economic trading conditions, the 2009 Expo has been cancelled.
(London)
Current Economic Downturn

- Watch more closely for red flags
  - Greater outsourcing and globalization to save money may create even greater risks
  - Include smaller providers not just the larger ones
- Revisit your risk assessment
  - Identify new or increased risks
- Revisit your business impact analysis
  - Protect critical functions from cutbacks and elimination
  - Review supply chain map for changes
- Retain those who perform critical functions
  - Consideration in employee downsizing
The right hand doesn’t know...
Need to Avoid a Silo Approach

- Organizations are symbiotic and each business unit supports all others
  - Critical operations in each business unit must be functional
- Business continuity planning is a core business practice
- Business continuity planning for the supply chain is not a separate, independent planning activity
Who Protects the Company

- Business Continuity
- Disaster Recovery
- Risk Management
- Emergency Response
- Crisis Communications
- Security
- Health & Safety
- Quality Management
- Environmental Management
Three Possible Approaches

- Create/maintain separate silos – individual departments/programs
- Create/define shared responsibility; some integrated functionality
- Central management for all related functions
A Holistic, Unifying Approach

One Department

Reports to executive management, e.g., Vice President of Enterprise Risk Management, or headed by executive level position, e.g., Chief Risk Officer
Regulatory Requirements

- We all have them
- Most prevalent in financial and health industries
- Disaster Recovery Journal (DRJ)
  - Headed by Martin Myers, Business Continuity Manager, Card Services Division, Bank of America.
  - Initial spreadsheet = 121 entries
  - “...realized that our list will never truly be complete, and as long as there are lawmakers and bureaucrats, new laws will be added.”
Other

- **Gramm-Leach-Bliley Act (GLBA)**
  - Federal Trade Commission—requires written information security program

- **Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule**
  - Department of Health & Human Services—requires integrity and protection of all forms of health information

- **Sarbanes-Oxley Act (SOX)**
  - Securities & Exchange Commission—requires infrastructure to preserve and protect information, records, and data

- **Six Sigma**
  - Elements of Business Continuity Planning /Disaster Recovery Planning are process-oriented disciplines; quality improvement process may apply

- **Federal Acquisition Regulations (FAR)**
  - Requirements vary by solicitation.
  - Ability to perform during a disaster could reasonably be a requirement for some products or services.
Voluntary Certification

- Involves a comprehensive substantiation of conformity to all the applicable requirements of the standard(s).
- Demonstrates that all elements of the standard have been addressed.
- Certification is:
  - Process based
  - Focus on risk control
  - Require documentation
  - Require ongoing review and improvement
Value of Voluntary Certification

- Simplifies validation of suppliers’ business continuity capability
- Provides a standard measure to compare potential suppliers
- Provides guidelines and methodologies for developing and maintaining a Business Continuity Program
- Competitive advantage for certificate holder
Why Become Certified?

- Visible demonstration of commitment to business continuity
- Standardized validation to all stakeholders regarding the viability of your program
- Ease in responding to audit requests and other inquiries
- *Possible* insurance premium savings and credit rating enhancement
Possible Issues

- For Suppliers: Multiple customers applying different standards
- Possible potential legal ramifications
- You do not make a hog fatter by weighing it.” (Quoted in the Sloan Report)

Dissenting Voice:
“The last thing businesses need is additional regulatory interference. Business continuity is a good example of stewardship. There are good stewards and there are bad stewards. If a company should fall victim to their own poor stewardship and go out of business as a result, so be it. That's capitalism for you.”
Business Continuity Guidelines

**Business Continuity Standards**


Title IX, Public Law 110-5, 2007: Section 524 directs Secretary of DHS to establish and implement a “Voluntary Private Sector Preparedness Accreditation and Certification Program” (PS-Prep)

And others...for example
- Canadian Standards Association (CSA) Z1600 Emergency Management & Business Continuity Programs
- Singapore Business Federation: Technical Reference for Business Continuity

- Charged by DHS with developing, implementing and administering the accreditation and certification program.
- To establish and oversee the development and implementation of the accreditation and certification requirements of Title IX of PL 110–53
References / Reading

- Sloan Report: Framework for Voluntary Preparedness includes extensive crosswalk of standards, guidelines, best practices (1/18/08) www.nyu.edu/intercep

  http://news.thomasnet.com/companystory/550697 or visit ANSI Public Documents Library www.ansi.org

- ASIS Press Release (10/15/08): “ASIS is seeking key input from business continuity professionals to develop potential membership on the technical committee that would draft and critique the new standard...Interested parties may contact ASIS at: guidelines@asisonline.org ”