BC9: Continuity & Resiliency
Paradigm and Proliferation

Roger Stearns  MBCI, CBCP, CHS-III
Fidelity Investments
Thomas Kuhn’s 1962 book *The Structure of Scientific Revolutions*. Kuhn used optical illusion to demonstrate the way in which a paradigm shift could cause one to see the same information in an entirely different way.
Overview

This session will discuss business continuity, the rapid growth of various planning models, and requirements and regulations driving the industry today. It will also look at the influencers and effects they have on business today.

- Definitions
- Timelines
- Drivers
- Convergence
- Drivers

How many legs does this elephant have?
Definitions

**Continuity:** uninterrupted connection, succession, or union; uninterrupted duration

**Resiliency:** an ability to recover from or adjust easily to misfortune or change
Definitions Cont.

**Paradigm:** A set of assumptions, concepts, values, and practices that constitutes a way of viewing reality for the community that shares them

**Proliferate:** to grow by rapid production; to increase in number
Definitions Cont.

**Asymmetrical:** lack of proportion, ill-proportioned

**Convergence:** the act of converging and especially moving toward union or uniformity; independent development of similar characters often associated with similarity.
Key dates for a profession

2007       BS 25999 Part Two
2005       BS 25999 Part One
2004       U.S. SEC approves NASD Rule 3510, 3520 and NYSE Rule 446
2003       Northeastern US Blackout
2002       Sarbanes-Oxley Act
2001       Gramm-Leach-Bliley Act goes into effect
2001       9-11 Terrorist attacks (NYC, Washington DC.)
2000       NFPA 1600 is published

1997       FFIEC declares, board of directors are responsible if recovery plans for distributed computing environments are not in place
1997       JCAHO publishes information security, emergency preparedness, and recovery planning in the health care field
1996       U.S. Health Dept. forms HIPAA
1990       Organizations recognize the need for operational recovery, not just data recovery.
1989       U.S. FFIEC requires documentation, maintenance, and testing of recovery plans
1988       Black Tuesday. Market crash
1983       U.S. OCC requires financial institutions to develop documented recovery plans
1970       Hot site market emerges as companies begin contracting with alternate site vendors or disaster recovery
1960       Reliance on data increases; frequency of backup and storage increases from weeks to days
1950       Companies begin storing backup copies of their critical records
Industry Evolution


IS / IT

Security

Disaster Recovery

Contingency

Continuity

IT Continuity

Resiliency

• Use older equipment as newer come in
• Up front cost is cheap ($)
• Technology to maintain 2 environments ($$$)
• Usability / Functionality (LOW)
• Operational Recovery (1-30%)

• Use equipment = to production
• Up front cost can be expensive ($$$)
• Technology to maintain 2 Locations ($) 
• Usability / Functionality (HIGH)
• Operational Recovery (30-100%)

• Its all production
• Up front cost . Multi site operations
• Technology to maintain 2 Locations (<$)
• Operational Recovery ( 100%)
How do you want to recover?
(Ex. Loss of facility/production site)
Convergence of Risk

- Plethora of regulations and guidelines
- Staffing
- Leadership
- Common language
- Metrics & Reporting
Asymmetrical Processing

- Single sited
- Centers of Excellence
- S-P-O-F
- 70/30, 80/20, 90/10 Splits
- Secondary Production Sites
- Alternate Work Sites
Business Continuity Drivers
Presidential Directives
Continuity of Government

George W. Bush Administration

Clinton Administration
- "Federal Response Plan" [FEMA 9230.1-PL], April 1999

George H. W. Bush Administration

Reagan Administration
- Executive Order 12656, "Assignment of Emergency Preparedness Responsibilities", November 18, 1988
- Section 202 The head of each Federal department and agency shall ensure the continuity of essential functions in any national security emergency by providing for: succession to office and emergency delegation of authority in accordance with applicable law; safekeeping of essential resources, facilities, and records; and establishment of emergency operating capabilities.
- NSD 69 NSDD 55, "Enduring National Leadership" September 14, 1982

Carter Administration

Truman Administration
- National Security Act of 1947, July 26, 1947
Industry Regulations

- NFPA 1600 (US), CZ 1600 (CA)
- Sarbanes Oxley Section 404
- FINRA/NASD 3510
- FINRA/NASD 3520
- NYSE Rule 446
- OMB Circular A-130
- HIPAA
- BASEL II
- FFIEC
- NIST 800-34
- ISO/BC 17799
- FDA 21 CFR 11
- FCPA
- 38A 1
- HB 221 – 2004
- HB 292 – 2006

Etc....
Boards & CEO’s

- Response to investors
- Response to Regulators
- Response to Audits
- Regulations
Establishing Continuity Governance

**Corporate Governance**
- Provide Strategic Leadership
- Provide Policy & Framework
- Provide Oversight
- Make Decisions

**BU Governance**
- Assesses BU Risk
  - Reviews BIA’s
  - Formulates Strategies
  - Reports issues
  - Make BU Decisions

**Planning & Control**
- Conduct BIA’s
  - Build Strategies
  - Build Plans
  - Build Call Lists
  - Test Plans

---

**BU Mgmt.**
- BU Mgmt.
- Application PM’s
- BU Rep / Champs
- Functional Mgr.

**Functional**
- BCP’s
- BU Rep / Champs
- BIA’s

**Technical**
- BCP’s
- Technical Leads

---

**Legal**
- Compliance
- Risk
- Continuity
- Facilities
- IT / IS
- Regulatory
- Audit
ROI of Resiliency

- **Remote Access**
  With a business resiliency solution, companies can integrate a remote access solution, enabling employees to receive always-available access to the information they need at any time and place. This can include redundant connections to core business applications, individual employee documents, emergency response plans, CRM functions, current email, and legacy applications. An organization can also use remote accessibility to save on real estate costs through employee telecommuting and better supporting a mobile workforce.

- **Collaboration Tools**
  People and partners can be integrated into a collaborative environment with dynamic access and delivery of critical information. With everyone working together using the same data and tools, including instant messaging, team workplaces, contact directories, and e-meetings, improved collaboration will greatly increase productivity throughout the organization.

- **Single Point of Access**
  With a business resiliency infrastructure, organizations can operate on a single point of personalized interaction with information, applications, people, and processes, for a unified user experience. Scalable and reliable portals that extend a user’s workplace to any browser or desktop are a must for a resilient organization. Users can view, create, and edit basic documents, spreadsheets, and presentations from within the portal for simple yet controlled access.

- **Misc.**
  1) System features like faster and better-qualified decision making through increased access to critical information
  2) Lower costs through self-service of human resource–related functions.
  3) Decreased IT help desk costs through better distribution of timely information.
  4) Telecommuting and thus lower real estate cost.
Homeland Security Presidential Declarations (HSPD)

**HSPD 5**
- Develop a National Response Plan that integrates all existing federal response plans.
- “Domestic Incidents”
- Create a National Incident Management System (NIMS)

**HSPD 7**
Enhance the protection infrastructure and key resources against terrorist acts that could: damage the private sector's capability to ensure the orderly functioning of the economy and delivery of essential services.

**HSPD 8**
To ensure the preparedness of the Nation to prevent, respond to, and recover threatened and actual domestic terrorist attacks, major disasters, and other emergencies. All hazard Planning.

**Title IX, H.R 1**
Voluntary preparedness standards for Private Sector Preparedness. Regulatory vs. Standards And verification
FEMA
The Four Pillars

- NIMS
- NRP
10 Practices

- Project Initiation and Management
- Risk Evaluation and Control
- Business Impact Analysis
- Developing Business Continuity Strategies
- Emergency Response and Operations
- Developing and Implementing Business Continuity Plans
- Awareness Programs and Training
- Maintaining and Exercising the Business Continuity Plans
- Crisis Communications
- Coordination with External Agencies

Seven-Step Model

Step 1 - Project Initiation Phase
  Objectives and Assumptions

Step 2 - Functional Requirements Phase
  Fact Gathering, Alternatives, and Decisions by Management

Step 3 - Design and Development Phase
  Designing the Plan

Step 4 - Implementation Phase
  Creating the Plan

Step 5 - Testing and Exercising Phase
  Post Implementation Plan Review

Step 6 - Maintenance and Updating Phase
  Updating the Plan

http://www.drii.org/DRII/
BCI

Good Practices Guide

Section 1  BCM Policy & Program Management
Section 2  Understanding the Organization
Section 3  Determining BCM Strategy
Section 4  Developing and Implementing BCM Response
Section 5  Exercising, Maintaining & Reviewing BCM arrangements
Section 6  Embedding BCM in the Organizational Culture

http://www.thebci.org/
Continuity management is the process by which plans are put in place and managed to ensure that IT Services can recover and continue should a serious incident occur. It is not just about reactive measures, but also about proactive measures - reducing the risk of a disaster in the first instance.

Continuity management is regarded as the recovery of the IT infrastructure used to deliver IT Services, but many businesses these days practice the much further reaching process of Business Continuity Planning (BCP), to ensure that the whole end-to-end business process can continue should a serious incident occur. (1990’s)

http://www.itlibrary.org/
ISO/IEC 20000

Manage Services

Management Responsibility

PLAN
Plan Service Management

ACT
Continuous Improvement

CHECK
Monitor, Measure & Review

DO
Implement Service Management

Business Requirements

Customer Requirements

Request for new or Changed Services

Other business, process, customer, suppliers

Other Teams (ex. Security)

Business Results

Customer Satisfaction

New or Changes Services

Other business, process, customer, suppliers

Teams & People Satisfaction

http://www.iso.org/iso/catalogue_detail?csnumber=41332
FFIEC
Planning Model

**Business Impact Analysis**
- Threats
- Impacts

**Risk Assessment**
- Probability
- Priority

**Risk Management**
- Business Continuity Plan
  - Specific
  - Flexible
  - Focused
  - Effective

**Risk Monitoring**
- Testing
- Reporting

The FFIEC BCP Booklet replaces the existing Chapter 10 of the 1996 IS Examination Manual entitled *Corporate Contingency Planning*.

**FFIEC** also places more emphasis on testing and updating business continuity plans by using the Four basic points of 1) BIA, 2) Risk Assessment, 3) Risk Management, and 4) Risk Monitoring.

This process acknowledges the current rate of change in today’s planning environment including But not limited to Technology, Organization, RTO’s, Costs/ROI. (March 2003)

[FFIEC logo]

http://www.ffiec.gov/
NASD 3510

Directs Financial firms to have plans containing:

1. Data back-up and recovery (hard copy and electronic)
2. All mission critical systems
3. Financial and operational assessments
4. Alternate communications between the member and its customers
5. Alternate communications between the member and its employees
6. Alternate physical location of employees
7. Critical business constituent, bank, and counter-party impact
8. Regulatory reporting
9. Communications with regulators
10. How the member will assure customers’ prompt access to their funds and securities in the event that the member determines that it is unable to continue its business.

Each member’s plan must address the listed categories only to the extent applicable and necessary. At the same time, the above-listed categories are not exhaustive; members should address other key areas for their plans to be complete and thorough based on their business and operations.

Rule 3510(b) requires each member to update its plan in the event of any material change to the member’s operations, structure, business, or location. Each member must also conduct an annual review of its plan to determine if any updates are needed in light of any changes to the member’s operations, structure, business, or location. (August 2004)

http://www.finra.org/index.htm
The BC Guideline is a tool to allow organizations to consider the factors and steps necessary to prepare for a crisis (disaster or emergency) so that it can manage and survive the crisis and take all appropriate actions to help ensure the organization’s continued viability.

The advisory portion of the guideline is divided into two parts: (1) the planning process and (2) successful implementation and maintenance. Part One provides step-by-step Business Continuity Plan preparation and activation guidance, including readiness, prevention, response, and recovery/resumption. Part Two details those tasks required for the Business Continuity Plan to be maintained as a living document, changing and growing with the organization and remaining relevant and executable. (Jan. 2005)
BS 25999
Continuity Planning Framework

BS 25999 Part-1 & 2: outlines the continuous lifecycle of the business continuity management system, defining the system as a living and continuously evolving program (April 2007, Nov 2007)
A wide range of terminology has been used to describe the processes associated with managing disruptions. Some of these terms include:

- Business continuity planning;
- Continuity planning;
- Contingency planning;
- Crisis management;
- Disaster recovery planning;
- Emergency management;
- Incident management;
- Disruption management;
- Business resumption planning; and
- Business resilience.
The program elements shall be applicable to prevention, mitigation, preparedness, response, and recovery.

- The program shall comply with applicable legislation, policies, regulatory requirements, and directives.

- The entity shall implement a strategy for addressing the need for revisions to legislation, regulations, directives, policies, and industry codes of practice.

- The entity shall identify hazards, monitor those hazards, the likelihood of their occurrence, and the vulnerability of people, property, the environment, and the entity itself to those hazards. (1995, revised 2007)
Cross-Walk Exercise

<table>
<thead>
<tr>
<th>REGULATIONS &amp; GUIDELINES</th>
<th>Subject areas</th>
</tr>
</thead>
<tbody>
<tr>
<td>HSPD / FEMA</td>
<td>✓</td>
</tr>
<tr>
<td>DRII / BCI</td>
<td>✓ ✓</td>
</tr>
<tr>
<td>ITIL</td>
<td></td>
</tr>
<tr>
<td>ISO 20000</td>
<td></td>
</tr>
<tr>
<td>FFIEC</td>
<td></td>
</tr>
<tr>
<td>FINRA/NASD 3510</td>
<td>✓ ✓ ✓</td>
</tr>
<tr>
<td>ASIS</td>
<td></td>
</tr>
<tr>
<td>BS 25999</td>
<td>✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>NFPA 1600 / CZ 1600</td>
<td>✓ ✓ ✓ ✓ ✓ ✓ ✓</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Risk Analysis</th>
<th>BIA</th>
<th>Strategies</th>
<th>BC Plan</th>
<th>Exercising</th>
<th>Reporting</th>
<th>Approvals</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
What has changed
Where is the bar?

**Traditional Impact model:** Although positioned well, the Low/High incidents are rare, but could have major employee availability issues. Stability of resources in High/Low incident category are a major advantage.

**Higher Frequency of High impact events:** The model follows the standard pyramid shape. However, the frequency of Low/High incidents is much greater than the traditional model. Also, the High/Low area seem to be more resilient do to the increase in risk mitigation as a result of higher frequency.
Natural Disaster

- Recent increase in events
- Scale and frequency
- More people looking to Government & Business to increase recovery capability

1. Are the events worse?
2. Are we less tolerant?
3. Is this the effect of development in risk prone areas?
Hurricane Strikes vs Population for Broward, Florida

Legend:
- **X**: Hurricane Category 1-2
- **X**: Hurricane Category 3-5
- **X**: Storm moving faster than 30 m.p.h.
- **Direct Strike**
- **Indirect Strike**
- Conventional Landfall Storm (Moving from water to land)
- Exiting or Inland Storm (Moving from land to water)
Hurricane Strikes vs Population for Galveston, Texas

Legend:
- **X** Hurricane Category 1-2
- **X** Hurricane Category 3-5
- **X** Storm moving faster than 30 m.p.h.
- **Red Line** Direct Strike
- **Green Line** Indirect Strike
- **Conventional Landfall Storm** (Moving from water to land)
- **Exiting or Inland Storm** (Moving from land to water)

Decade:
- 1900
- 1910
- 1920
- 1930
- 1940
- 1950
- 1960
- 1970
- 1980
- 1990
- 2000
- 2010

Population:
- 0
- 20,000
- 40,000
- 60,000
- 80,000
- 100,000
- 120,000
- 140,000
- 160,000
- 180,000
- 200,000
- 220,000
- 240,000
- 260,000
- 280,000
Global Warming

- Island Effect
- Heat banks
- Smog