Business Resiliency

“Tomorrow …
is not the time to find out that
I can’t continue critical business functions”
Agenda

Overview & Objectives

Evolution and Definitions of “Resiliency”

A Business Case for BCM

Questions ALL Organizations need to address

Costs – Risks – Impacts

10 Things Learned about Business Resiliency

Q&A
Overview

• Due to recent events, Business Resiliency is at the forefront of Corporate Governance:
  
  – Natural Disasters:
    – floods, tsunami, earthquakes, hurricanes
  
  – Man Made:
    – 9/11, Terrorism, Gulf Oil Spill, Cyber Attacks, …

• Compliance and Corporate Governance:
  
  – IT Business Resiliency helps ensure compliance with recently implemented legislation and/or amended laws

2 of 5 enterprises that experience a disaster will go out of business in five years. (Gartner)
Are you prepared if the big one does hit?  1.5 min video

A little wave of disruption …little problem,
A BIG WAVE of disruption ………
Do you have more than a surf board for Recovery?
BCM Objectives

- Limit severity of the event and the magnitude of loss
- Minimize extent of the interruption & decision making during a crisis
- Identify critical resources & functions
- Define a process to protect critical resources
- Define alternatives for continuing critical functions
- Train personnel
- Continual review and maintenance
- Integration of Business Continuity with Enterprise Strategic Planning
Regs & Standards that have DR/BCP references

**All**
- Sarbanes-Oxley Act of 2002
- The Foreign Corrupt Practices Act
- Emergency Planning and Community Right-to-Know Act of 1986
- NFPA 1600 (Standard)
- ISO 27001

**Financial and Banking**
- Dodd Frank
- The New Basel Capital Accord
- NASD & NYSE Proposed Regulation
- FFIEC BCP Handbook
- NCUA Letter To Credit Unions
- Financial Modernization Act of 1999
- Interagency White Paper on Sound Practices to Strengthen the Resilience of the US Financial System
- Expedited Funds Availability Act
- Various OCC Comptroller’s Handbooks
- Financial Services and Market Act

**Food and Pharmaceutical**
- FDA Code of Federal Regulations, Title XXI

**Government**
- Presidential Decision Directive 67 & 63
- Executive Order 12656
- Office of Management and Budget (OMB) Circular A-130
- NIST’s Contingency Planning Guide for Information Technology Systems (Standard)

**Healthcare**
- Health Insurance Portability and Accountability Act

**Service Organizations**
- Statement on Auditing Standards (SAS) 70 audit reports

**Telecommunications**
- Telecommunications Act of 1996
- Executive Order 12472

**Utilities**
- State Public Utilities Codes
Evolution of DR / BCP / BCM

1964
- IBM introduces OS/360
- Data Processing mainframe centric

1970’s
- Development of Ethernet

1973
- Novell introduces first NOS

1981
- 10Mb Ethernet
- First PC - DOS

1983
- Government allows commercial email on internet (MCI)

1989
- Laptops & Notebooks

1990
- First Browsers
- Mosaic

1991
- Netscape

1993-4
- Development of WWW

1995-2005
- E-Commerce
- E-Business
- Wireless Mobile Computing
- Electronic vaulting, NAS, SANS

2010-....
- Cloud Computing

DRP | DRP + | BCP | BCM
<table>
<thead>
<tr>
<th>Disaster Recovery Plan: (DRP)</th>
<th>Document defining the IT resources (hardware, software, communications, data), actions and tasks required to recover the infrastructure needed to support the business functions</th>
<th>IT Centric</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Continuity Plan: (BCP)</td>
<td>Document defining the advance planning &amp; preparations that are necessary to minimize loss and ensure continuity of the critical business functions of an organization in the event of disruption</td>
<td>Business Centric - Encompasses DRP</td>
</tr>
<tr>
<td>Business Continuity Management: (BCM)</td>
<td>Management strategies, processes and techniques which seek to provide the means for continuous operation of the essential business functions under all circumstances</td>
<td>Governance; Encompasses BCP &amp; DRP, integrating the strategic processes of the enterprise</td>
</tr>
</tbody>
</table>
Many organizations champion or develop their own BCM/BCP methodologies:

- DRII – Disaster Recovery Institute International supports a methodology comprised of 10 core practices:
  1. Project Initiation and Management
  2. Risk Evaluation and Control
  3. Business Impact Analysis
  4. Developing Business Continuity Strategies
  5. Emergency Response and Operations
  6. Developing and Implementing Business Continuity Plans
  7. Awareness and Training
  8. Maintaining and Exercising Business Continuity Plans
  10. Coordination with Public Authorities
BCI - Business Continuity Institute

supports a methodology comprised of 6 core stages

1. Understanding Your Business (BIA / RA)
2. Business Continuity Management Strategies
3. Develop and Implement Business Continuity Response
   a. Business Continuity Plans
   b. Resource Recovery Solutions and Plans
   c. Crisis Management Plans
4. Building and Embedding a Continuity Culture
   a. BCM Culture and Awareness Program
   b. BCM Training Program
5. Exercise Maintenance and Audit
6. Program Management (Project Mgt & Policy)
Business Case for having BCM Program

Standard & Poor's (S&P) evaluates the enterprise risk management (ERM) capabilities of non-financial companies that it covers.

Extrapolating an ERM evaluation to a logical, eventual conclusion, if a company didn't have a BCM program, it’s credit rating could be lowered.

The consequence? Borrowing money would cost more, and for the large companies that S&P reviews, that could be a material consequence.

S&P already evaluates risk management at banks, insurance, energy and agribusiness companies, and now wants to do so for companies in other sectors.
Business Case for having BCM Program

- Suppose one of those companies wanted to issue a bond for $200 million to build a new plant.

- Suppose also that, due in part to its assessment of the company’s risk management, S&P lowered the company's credit rating from, say, **A- (upper medium grade)** to **BBB+ (lower medium grade)**.

  - As a result, the company is forced to pay a **4.1 %** coupon instead of **3.9%** to make the bond attractive to investors or underwriters.

  - Based on US$200 million, two-tenths of 1% (the difference between 4.1% and 3.9 %) is US **$400,000**.

- Next ………>
Business Case for having BCM Program

Questions these scenarios raise:

– **What could you do for $400K?**

– **Could you develop a company BCM program for $400K?**

– **Could you hire an experienced, certified BCP professional to run it for $400K? Set up a recovery site?**

– **Could you make a company genuinely more resilient--and therefore more credit-worthy -- for $400K?**
What is Business Continuity Management?

A process designed to reduce an organization’s risk of unplanned interruptions to key business functions, thus minimizing the impact and ensuring the continuity of critical business services.
Why is Business Continuity Management Relevant?

Organizations seek to mitigate “deadly” risks associated with:

1. Business process failure
2. Harm to personnel on site
3. Loss of revenues, customers or business opportunities
4. Negative impact to brand or public image
5. Legal and regulatory issues
Failing to Plan = Planning to Fail

25% of all businesses never reopen after a disaster.

Source: www.ready.gov
What are the benefits of a BCM plan?

- Limit the magnitude of loss
- Limit the severity and extent of interruption
- Provide alternatives for continuing critical business functions
- Minimize the decision-making process during a crisis
- Establish a plan for the recovery and restoration of business operations
- Develop personnel trained to efficiently and effectively maintain the business even under adverse circumstances
Potential Threats (Causes)

**Natural**
- Hurricanes
- Earthquakes
- Floods
- Tornadoes
- Winter storms
- Hail
- Wildfires
- Pandemic

**Man-Made**
- Fires
- Computer viruses
- Break-ins
- Vandalism
- Terrorism
- Fraud
- Hazardous material spill
- Disgruntled employee
- Nuclear plant incident

**Technological**
- Power outage
- System failure
- Software failure
- Network failure
- Facility failure
- Viruses, worms, Trojan horses
- Hackers
- Hardware failure

Threats may also impact your business indirectly by disrupting your suppliers, third party service providers, or customers.
Cost of Being Down by Industry

$ Costs of Data Loss

With no access to systems, financial losses can accumulate quickly. The chart below outlines the costs associated with computer downtime and lost data for businesses.

<table>
<thead>
<tr>
<th>Industry Sector</th>
<th>Lost Revenue Per Hour</th>
</tr>
</thead>
<tbody>
<tr>
<td>Energy</td>
<td>$2.8 million</td>
</tr>
<tr>
<td>Telecommunications</td>
<td>$2.0 million</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>$1.6 million</td>
</tr>
<tr>
<td>Financial Institutions</td>
<td>$1.4 million</td>
</tr>
<tr>
<td>Information Technology</td>
<td>$1.3 million</td>
</tr>
<tr>
<td>Insurance</td>
<td>$1.2 million</td>
</tr>
<tr>
<td>Retail</td>
<td>$1.1 million</td>
</tr>
<tr>
<td>Pharmaceuticals</td>
<td>$1.0 million</td>
</tr>
</tbody>
</table>

One Study showed 54% of surveyed businesses indicated 1 hour of downtime would cost $51K - $1M

Same survey found the avg restore, access & availability to critical systems would take 9-12 hours

Source: http://www.ontrack.com/understandingdataloss/
Cost of Being Down by business indicators

Know your downtime costs by Hour, Day and Week ...

Productivity
- # Employees affected
  x hours out
  x burdened hourly rate

Damaged Reputation
- Customers; Suppliers;
  Financial Markets;
  Banks; Business Partners

Revenue
- Direct Loss; Compensatory Payments;
  Lost Future Revenue; Billing Losses;
  Investment Issues

Financial Performance
- Revenue recognition; Cash Flow;
  Lost Documents (A/P); Payment
  Guarantees; Stock Price

Source: Gardner
Risk Assessment

Consider threats and vulnerabilities for all critical assets:

• People

• Data

• Software (operating systems, applications, etc.)

• Infrastructure Equipment
  (PCs, distributed systems, mid-range, mainframe, network, telecom, etc.)

• Building / facilities / environmental
  (power, HVAC, physical security)

• Inventory and materials

• Production and plant equipment
Business Impact Analysis

Identifies the impact resulting from disruptions to both primary and secondary business functions.

• **BIA helps:**
  – predict disastrous effects and
  – define single points of dependency or failure

• **BIA Identifies**
  – RTOs - Recovery Time Objectives &
  – RPOs - Recovery Point Objectives

• **BIA Focus:** (People, Process, Technology)
  – Personnel/vendors
  – Critical business functions
  – Critical records/service internal/external
  – Infrastructure – telecom/communications
  – Applications
Incident Action Plan (IAP) Considerations:

- **Incident goals** (where the response system wants to be at the end of response)
- **Operational period objectives** (major areas that must be addressed in the specified operational period to achieve the goals or control objectives)
- **Response strategies** (priorities & general approach to accomplish the objectives)
- **Response tactics** (methods developed by Operations to achieve the objectives)
- **Organization list** showing primary roles and relationships
- **Assignment list** with specific tasks
- **Critical situation updates and assessments**
- **Composite resource status updates**
- **Health and safety plan** (to prevent responder injury or illness)
- **Communications plan** (how functional areas can exchange information)
- **Logistics plan** (e.g. procedures to support Operations with equipment, supplies, etc.)
- **Responder medical plan** (providing direction for care to responders)
- **Incident map** (i.e., map of incident scene)
- **Additional component plans**, as indicated by the incident.
What needs to be in place

1. IT Business Resiliency should be conducted on an *enterprise wide* basis

2. A thorough *Risk Assessment, BIA and Incident Action Plan* is foundational to this effort

3. IT Business Resiliency is *more than* the recovery of the technology; *(it is the recovery of the business)*

4. The effectiveness of IT Business Resiliency *can only be* validated through thorough *testing*

5. Business continuity plans and test results should be subjected to an *independent assessment*

6. Business continuity plans should be *periodically updated* to reflect and respond to *changes* in the institution
What are some of the Danger Signs?

- Effort is under estimated
- Recovery requirements not adequately defined
- Restoration process not thought through
- Business Continuity Manager not recognized as a key organizational position
- Inadequate plan maintenance and testing
- Viewed as a project and not a process
- Not achieving Sr Management “buy-in”
Corporate Responsibility/Sponsorship

Business Continuity is not just a phase or project to be implemented when time & resources allow.

It is an ongoing program implemented to protect data, and ensure the integrity and security of the total business, facilities, information and the well-being of employees, which is of paramount importance.
Questions You Need to be Asking

• **What** systems do you expect to be available, and when?

• **What** systems do you rely on and when would you need for them to be available?

• **Who’s responsible?** - Are these expectations clearly documented in the recovery plan?

• **When** was this plan last reviewed by you?

• **How** will the business function in the interim?
BCM Maturity Model - Where are you?

What business continuity requirements does your company have to comply with?

- OSFI
- SEC
- GLBA
- CFR 11
- Basel II
- OTS
- NAIC
- IDA
- NASDAQ
- HIPAA – 21
- FDIC
- DoD

Level - Maturity

0 – Non-existent
1 – Initial /ad hoc
2 - Repeatable, but intuitive
3 - Defined process
4 - Managed and measurable
5 – Optimized
Senior Management Vested Interest

- Benefits the company and the bottom line
- Provides improved lines of communication
- What you don’t know CAN hurt you
- Selling point to customers and business partners
- Alternative use of recovery resources (e.g., training facility)
- Awareness of potential effects (e.g., supply chain vulnerabilities)

- ABOVE ALL — Fiduciary responsibility!
In Summary – Making the Methodology Work

- **Identify** your business processes

- **Focus** on *critical* business processes first

- **Ensure** Business Continuity Planning is a corporate wide initiative

- **Coordinate** with IT and other business units that support and interface with your operation

- **Prepare** now so that critical decisions can be made and proper steps taken while there is time to do so
10 things we have learned about Business Resiliency!

1. People support & “celebrate” what they help create
2. BCM is not the same as Disaster Recovery
3. BCM is not just about the plans
4. BCM can help differentiate companies
5. Implementing BCM can save you money across the business
6. Having good BCM is great for your reputation even after an adverse event
7. Your IT infrastructure costs may be too high
8. Insurance may not cover all your losses
9. Lower insurance premiums possible
10. It’s a very security conscious thing to do!

“A good Business Continuity Plan is tested.
“No battle plan ever survives contact with the enemy.”:
Field Marshall - Bernard von Moltke
When was the last time someone reviewed your plan?
Learning Objectives

Objective 1 –

Raise awareness of rules, regulations and trends that impact an organization during an outage.

Objective 2 –

To provide thoughts and action plans to address Business Resiliency as a key to long term corporate health and not just an insurance policy.
Thank You!
Any Questions?

Danny Shaw
SE Practice Leader, IT Risk Advisory Services
Experis
+1.404.586.2773 (o)
+1.678.910.4355 (m)
Danny.Shaw@experis.com