Session Overview

Presenter:
Michael J. Corby, CCP, CISSP, PMP
Senior Vice President & Practice Leader Business Continuity Risk Management, Marsh Risk Consulting

Summary:
This session will provide a brief overview of the components of a Business Continuity Risk Management Plan. Starting with a Business Impact Analysis that coincides with the creation of campus security and crisis response programs, it will address some quick and effective methods for identifying the technology components, processes, facilities, and key people that can assure a stable revenue stream, and can manage costs effectively despite events that can suddenly change the educational environment. The session will include discussion of how to provide consistent education for students, even when they are restricted from full campus access due to disease outbreak, damage to buildings or facilities, or major weather interruptions. In addition to providing education, the BCM process includes campus life concerns, faculty and staff management, continuation of research projects and grant proposals, and general community service obligations. Participants will understand the basics of Business Continuity Risk Management including how to assess key educational business components, the meaning of terms such as Recovery Time and Recovery Point Objectives, considerations for IT Disaster Recovery and establishing various Event Response and Management teams.

Why Business Continuity Risk Management

- Recent events (Tulane University, Louisiana State, etc) and relevant threats (weather, terrorist, violence on campus, health pandemics) are forcing many schools to focus on business continuity. Overall higher education has done very little beyond emergency management planning. The possibility of a catastrophic event is now very real to them.
- In fact, most universities lag far behind industry (financial services, manufacturing, healthcare, etc) that they are playing catch up to ensure that their institution survives a significant event.
- Many institutes of higher education could be severely impacted by a catastrophic event. Many universities (particularly private) run the risk of bankruptcy if they lose just one semester of tuition.
- Due to limited budgets, creative solutions are necessary to address new threats (partnering with other institutions, information technology, distance learning) and experienced outside consultants are sought after to address the risk.
- Limited budgets also drive the need to justify and prioritize alternate recovery strategies. Full redundancy for all functions and information technology is not an option.

What has Higher Education faced in the last few years?

- Storms, bombs, civil unrest, bad press, terrorism, crime, criminal use of technology, greek and athletic related incidents, foreign exchange problems, mismanagement, arson, conflicts of interest – just to name a few
- Each has the potential to be a major problem or disruption – with planning and exercising, many of these could also become minor incidents
- Being prepared is not just a nice-to-have – it is expected. Not being prepared for these foreseeable events is not an acceptable solution
- It’s much more than evacuation of a building. It’s keeping things running after that event (or in the terms of one university – its what to do once the fire truck leaves).

Are you Prepared to Respond?

What would be the impact on your Institution?

Key Concerns

- “In the past we planned for the loss of a building, should we plan for a campus-wide outage?”
- “I was able to recover from the last disruption, but my response exceeded the maximum allowable downtime. How can I accelerate recovery?”
- “I’m worried. Our faculty, buildings, students and technology are concentrated in a small area. How can I provide greater resiliency?”
- “Our students and faculty assume and expect that we protect their personal data. How do we implement and enforce the necessary policies and controls with the least amount of disruption to the operations?”
- “All we need is a business continuity plan. Why do I want you to conduct an impact analysis?”
- “A catastrophe would put me out of business. How do I develop a plan?”
- Our plan addresses only information technology. How do we ensure resiliency for people, facilities and equipment?”
Business Continuity Program

Three Important Components

- Financial operations, not tangible asset
  - Emergency Response
  - Business Continuity/IT Plans
  - Business Continuity/IT Plans

Graphical Representation of Emergency Response Elements

Purpose: Why are we concerned about Business Continuity?

Putting Response Protocols in Perspective

The Intensity Levels of the Individual Response Protocols

Three Important Components

- Physical, information security
  - Business Continuity
  - Business Continuity
  - Business Continuity

An Integrated Program

Business Continuity Planning—The Maturity Model
**The Impact on Finances (Revenue Loss)**

- Preparedness reduces the negative impact and speeds recovery
- Damage to financial results, reputation and key relationships

**The Impact on Reputation (Shareholder Value)**

- Effective crisis responses: +7 percent
- Ineffective crisis responses: -15 percent

**The Gap is Widening**

- Staying the same means going backwards
- Increasing Continuity Gap

**Business Continuity Programs**

- An organization’s ability to foresee, prevent, respond, and manage adverse risk and events
- A seamless solution so employees can focus on delivering services
- An approach that is:
  - Risk-aligned with the organizational goals
  - Balanced with both corporate needs and service locations
  - Standards based and validated
  - Program planning for ongoing preparedness
  - Sustainable through a maturity-model
  - Potentially self-funding
Business Continuity Solutions are designed to focus on existing plans...

Business Continuity Risk Management

**Periodic Re-Assessment**

- Business Partner Risk
- Pandemic Risk
- Environmental Risk
- Technology Risk
- Compliance Risk
- Other

**Event Response**

- Policies
- Strategy
- Governance
- Budget
- IT DR Plan
- Crisis Response
- Facility failover plan
- Compliance Mgt

---

**2008 - Business Continuity is all About Building a Dependable Revenue Stream**

"E. coli outbreak hits United States."

"Americans fear not getting paid after disaster."

"80 percent of businesses impacted by a disaster in New York said it cost them more than $100,000 a day."

"It is not a question whether or not the next Pandemic will break out, it is just a question when."

---

**The Methodology is a Cycle of Continuous Improvement**

**Business Continuity Management Evolution**

- Disaster recovery
- Recovery Time Objective (RTO) = Three days scenarios limited
- Y2K
- Contingency planning
- RTO = <24 hours
- Aftermath of Recent Incidents (9/11, VT, etc.)
- Incident management
- New scenarios

**Enterprise Risk Management (ERM)**

- Reduce and document incident costs
- Scale from minor incidents to large events
- Work with emergency services
- Meet safety & regulatory requirements
- Work with enterprise risk management
- Manage non-disaster Information Technology (IT) incidents

**High availability and incident management**

---

**A threat-based catastrophic planning approach has shown to be inefficient and difficult to achieve.**

A threat-based catastrophic planning approach has shown to be inefficient and difficult to achieve.

---

**Best Practice: an “IMPACT” - (versus a threat) - based approach**

Assume the resource is either unavailable for >30 days or, worst case, destroyed.

**Resources Impacted**

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Unavailable (total)</th>
<th>Unavailable (catastrophic)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pandemic</td>
<td>20% - 90% impact</td>
<td>20% - 90% destruction</td>
</tr>
<tr>
<td>Internal work force</td>
<td>30% - 70% impact</td>
<td>30% - 70% destruction</td>
</tr>
<tr>
<td>Students, faculty, contractors</td>
<td>30% - 70% impact</td>
<td>30% - 70% destruction</td>
</tr>
</tbody>
</table>

**Unavailability and Unrecovery for the Next 100 Years of Time**

- Pandemic: 80% or 90%
- Internal work force: 30% or 70%
- Students, faculty, contractors: 30% or 70%

**Key systems and their availability**

- Student records
- Financial records
- Employee records

**Any new technology (enhanced)**

**Prospective outcomes**

- Critical business processes
- Critical business functions
- Critical business information
- Critical business infrastructure

---

**Connecticut Conference of Independent Colleges**
Get Started by Focusing on Impacts
Identify where key elements of your revenue are “At Risk”

- STOP chasing threats – you could exhaust your resources looking for ways to mitigate or prevent each one
- START thinking about impacts – when they happen, they all have some impact on your organization
- PROTECT your organization by focusing on where the impacts would be most severe - you need to determine what parts of your organization are most critical and “at-risk”, then figure out ways to protect them

Impact Based Approach

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Analysis</td>
<td>Identify existing recovery strategies, tools, business issues, and gaps</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strategy</td>
<td>Identify critical process recovery times, financial impact from outage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plan</td>
<td>Select recovery strategy options, select strategy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Testing</td>
<td>Document recovery steps for business units</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Preparation</td>
<td>Train employees</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Resources should be mapped to critical processes

Address all dependencies and the skills required to maintain operations, whether a public entity, higher education provider, manufacturer, service company, or other type of organization

Process Overview

1. Develop BIA questionnaire using senior management’s recovery objectives
2. Conduct BIA workshop with business representatives
3. Distribute BIA and receive completed forms from business representatives
4. Review BIA questionnaire
5. Conduct follow-up interviews with business unit representatives

- Identify and document resource requirements based on BIAs
- Conduct gap analysis to determine gaps in recovery requirements and current capabilities
- Define recovery strategy options
- Select strategies

Execution: How do we go About Developing a BCRM Program?

Identifying Key Assets

**People**
- Students, Faculty, Visitors
- Specialized operations experts
- Families and Media
- Executives
- Administrators and At-large employees
- Consultants and specialists

**Process**
- Standard operating procedures
- Computer programs and data
- Validation and quality controls
- Automated processes
- Outsourced functions

**Technology**
- Central/departmental computers
- Desktop/laptop computers
- Network
- Voice communications
- Scanners/Point Of Sales (POS) devices
- Radio Frequency Identification (RFID) / Global Positioning System (GPS) / Wireless Devices (cell phones, PDA’s)
- Electronic ID and Financial cards
**Identifying Risks**

External drivers:
- Increased regulatory requirements
- Audit committees, Trustees, Board of Directors
- Business Partners and insurers
- Reliance on third parties (IT service providers)
- New threats and risks (violence, pandemic)
- Increased natural disasters

**Qualifying Risks**

<table>
<thead>
<tr>
<th>Impact</th>
<th>Likelihood</th>
<th>High risk</th>
<th>Medium risk</th>
<th>Low risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Low</td>
<td>Critical risks that potentially threaten the achievement of business objectives</td>
<td></td>
<td></td>
</tr>
<tr>
<td>High</td>
<td>Medium</td>
<td>Lower likelihood, but could have significant adverse impact on business objectives</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td>High</td>
<td>Lower likelihood, but more likely to occur</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td>Medium</td>
<td>Periodically reassess conditions to ensure ongoing alignment</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**The result of this approach is to focus on the key products or services that provide value**

- Segment (e.g., Undergraduate, Graduate, Continuing Ed., Distance Learning, etc.)
- Prioritize - Business: Reputation & Safety
- Select Prioritized Service or Product

**Business Impact Analysis solicits responses from many areas**

- Data collection worksheets
- To identify areas that represent the most substantial loss.

**Understanding the Internal Dependencies**

- *Sample Marsh Matrix from a Business Impact Analysis*

**Tactical Program Development Process**

- Identify single points of failure
- Identify business processes from compliance
- Quantify impacts and recovery times
- Identify inflows & outflows
- Identify interdependencies
- Refine their retention and back-up policies
- Develop recovery alternatives
- Investigate vendor solutions
- Document manual workarounds
- Develop data restore procedures
- List Vital Records and offsite locations
- Test solutions
- Integrate with Corporate Governance Program
- Update processes

---

**Organizational representative factors:**
- Risk
- Compliance
- Contingency plans
- Plans in detail
- Operations objectives

**Graduate, Continuing Ed.**

---

**Business Impact Analysis**

- Risk Management
- Information Systems
- Operations
- Accounts payable
- Organizational
- Management
Each department has to document their tolerance for disruption of their critical business processes, interdependencies, and recovery procedures.*

Data Center Strategies: No Single, “Right” Answer

Common strategies

Load sharing
Outsourcing/Disaster Recovery (DR)
Development and test
Production and standby

Less Expensive to Insourcing or Outsourcing?

Typical profile of economic value proposition of outsourcing solutions

Continuous availability
High availability

Typical profile of solution costs

Cost

Five Days
Three Days
48 Hours
24 Hours
Four Hours

Technologies to Reduce RTO/RPO

Assumes mirroring or shadowing plus a complete application environment
Database and/or file and/or object replication
Log/journal transfer (continuous or periodic)
Database and/or file and/or object backup

Electronically
Vaulting

Hot Standby or Load Balanced

Standard Recovery

Electronic Journaling

Hot Standby

12 hours
Disaster Recovery Time

48 hours
72 hours

12 minutes

Cost

Measuring Success

<table>
<thead>
<tr>
<th>Area under review</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Organization and structure</td>
<td>4421</td>
</tr>
<tr>
<td>2. Business impact analysis</td>
<td>3615</td>
</tr>
<tr>
<td>3. Strategy selection</td>
<td>3615</td>
</tr>
<tr>
<td>4. Plan documentation</td>
<td>4600</td>
</tr>
<tr>
<td>5. Awareness and testing</td>
<td>3742</td>
</tr>
<tr>
<td>6. Maintenance</td>
<td>4271</td>
</tr>
</tbody>
</table>


4. Plan documentation: Plan format: 8.00, Plan access: 8.00, Plan content: 8.00, Plan references and integration: 8.00.

5. Awareness and testing: Awareness programs: 8.00, Test criteria and objectives: 8.00, Test scripts: 8.00, Test execution and follow-up: 8.00.


Overall evaluation: 74.69.

Execution: Testing and Exercising the Plan Without Causing a Disaster
Options Available for Testing:
The Structured Walk-Through
Structured walk-through (“role-play”):
- Paper evaluation of a portion of a BC plan without the expenses or personnel resources associated with a full test
- Scope can vary from a review of a portion of the BCP to a review of the entire plan.
- Objectives:
  - Verify the contents of the plan;
  - Prepare for simulation testing;
  - Train new members and create employee awareness;
  - Maintain preparedness while limiting use of resources;
  - Affirm that the strategy documented in the plan is viable;
  - Educate critical personnel on their responsibilities in a disaster;
  - Confirm that the information in the plan is current and accurate; and
  - Identify areas of the plan that need revision or updates.
- Benefit is that it is cost-effective and non-invasive

Options Available for Testing:
Component Testing
- (Usually) an off-hours exercise to test a particular segment of the recovery plan.
- Differs from the structured walk-through in that it involves actual recovery activities
- Types of component tests include:
  - Emergency notification test (call tree tests);
  - Evacuation tests;
  - Data center or application recovery test;
  - Remote or dial-in access test; and
  - Critical business function recovery test.
- Objectives:
  - Demonstrate accuracy of the execution of the plan;
  - Verify the appropriate operating and incident escalation procedures;
  - Train and increase awareness of personnel; and
  - Validate previous modifications of the plan including the DRP.
- Benefit is that it is non-disruptive and focused

Options Available for Testing:
The Fully Mobilized “Drill”
Integrated simulation/full operations test:
- Performed at the actual recovery sites
- Utilizes the backup resources (i.e., AS 400 systems and workspace)
- Structured walk-through and/or a component test should precede
- Test transactions or replicated “live” transactions are processed
- Reports produced (actual results) should be reconciled against expected results
- Objectives:
  - Test entire plan or a portion of the plan under emergency scenarios;
  - Validate operational effectiveness and business unit interdependencies; and
  - Provide technical and administrative measurable results,
  - An exercise of this proportion is normally scheduled to take place after hours or during a weekend
- Benefit is that it requires inter-department coordination and is the best true test of the BCP

Collaborative Program Description
- Cooperative approach - allows for a single comprehensive approach based upon a model school template (which is developed during the pilot project of two or three institutions). The participating members will develop a unified program structure and approach, consistent strategies among the member locations and maximize internal (to the association) sharing of resources.
- Two Pilot Programs – Urban & Rural Campuses
- Utilize “Model School” based on information gained from the pilot programs for the remainder of the participating members
- Conducted one week event at each Phase 2 school which included a training session for the campus business continuity leader, several group workshops with the departments/colleges, and concluded with a walk-through exercise based on a scenario that Marsh presents.
- Sliding scale pricing model based upon the number of participants
The Collaborative Method

Business process and tolerances levels
- Engage representatives from:
  - Student Life
  - Academics
  - Administration
- Workshop sessions with data center management and Marsh
- Identify core applications, data dependencies, and applications in the data center
- Develop high-level gap analysis
- Develop current capability recovery timeline
- Verify recovery sequence and timeline with data center management
- Escalate observations with IT management
- Research commercially available recovery options

Current ITDR Capabilities
- Business process and tolerances levels

Next Steps
- Prepare gap analysis
- Decide on short-term recovery options
- Decide on long-term recovery options
- Develop:
  - Risk assessment
  - Gap
  - Continuity strategies recommendations
  - Continuity implementation plan
- Documented assessment report

Model School Template

Accessing and Completing the Department Business Continuity Plan

Business Impact Analysis (BIA) column is used to document recovery strategies for your business requirements. Estimated Time to Complete: 1 to 2 hours

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategy Development</td>
<td>Strategy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BCP Plan Development</td>
<td>Deploy plan development program for other essential business functions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BCP Policy &amp; Awareness</td>
<td>Develop policy statements</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Crisis Management</td>
<td>Develop escalation procedures, communications, roles and responsibilities, action steps</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Sample Marsh timeline for improvement

Michael J. Corby, Senior Vice President
Marsh, Inc.
200 Clarendon St.
Boston, MA 02116
Phone: (617) 421-0281
Mobile: (774) 452-4545
Email: michael.j.corby@marsh.com
Or your local contact from Marsh

www.marsh.com