Emergency Management Planning

Barbara Todd
Registrar, University of Colorado Boulder
RMACRAO Conference – July 17, 2013
Disasters are unexpected and can result in significant physical damage or destruction.
Some Are More Likely To Occur
So what makes us the most vulnerable?
Why Do We Need To Have Emergency Management Plans?

- Registrars, admissions, financial aid and/or enrollment management offices are critical to the mission of the institution, and any downtime can result in serious losses for the short- and long-term.
- Offices with developed plans, especially those who have tested the plans in mock operations, have been the most successful in recovering from a disaster.
Step 1: Begin with a Vulnerability Analysis

---

### Business Continuity and Recovery Plan

#### Vulnerability Analysis

<table>
<thead>
<tr>
<th>Impact</th>
<th>Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal</td>
<td>External</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type of Emergency</th>
<th>Probability</th>
<th>Human</th>
<th>Property</th>
<th>Business</th>
<th>Internal</th>
<th>External</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>High --&gt; Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 --&gt; 1</td>
</tr>
</tbody>
</table>
A Vulnerability Analysis...

- Allows you to identify your biggest area of risk.
- You can create specific business continuity plans that address the areas of largest risk.

What to do:
- Identify the probability of an emergency occurring – be creative. 5 is high; 1 is low.
- If this emergency occurred, what is the impact to human life, property and your ability to do business. Rate – 5 is high; 1 is low.
- If this emergency occurred, does your office or your institution (internal) or the community (external) have the resources to help you recover – weak resources = 5; strong resources = 1.
- TOTAL – add up the scores.
CU Boulder’s Risk Analysis

<table>
<thead>
<tr>
<th>TYPE OF EMERGENCY</th>
<th>PROBABILITY</th>
<th>HUMAN IMPACT</th>
<th>PROPERTY IMPACT</th>
<th>BUSINESS IMPACT</th>
<th>INTERNAL RESOURCES</th>
<th>EXTERNAL RESOURCES</th>
<th>TOTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power outage</td>
<td>5</td>
<td>1</td>
<td>2</td>
<td>5</td>
<td>5</td>
<td>1</td>
<td>19</td>
</tr>
<tr>
<td>Fire</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>6</td>
<td>5</td>
<td>1</td>
<td>20</td>
</tr>
<tr>
<td>Terrorism/Bomb</td>
<td>1</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>1</td>
<td>13</td>
</tr>
<tr>
<td>Protests</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>10</td>
</tr>
<tr>
<td>Snowstorms</td>
<td>5</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Tornado</td>
<td>2</td>
<td>1</td>
<td>5</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>Flood</td>
<td>1</td>
<td>1</td>
<td>5</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Disease outbreak</td>
<td>3</td>
<td>4</td>
<td>1</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>18</td>
</tr>
<tr>
<td>Indiv shooter/hostile</td>
<td>2</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>4</td>
<td>1</td>
<td>28</td>
</tr>
<tr>
<td>High winds</td>
<td>3</td>
<td>1</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>1</td>
<td>12</td>
</tr>
<tr>
<td>Haz Mat - loss of heat</td>
<td>2</td>
<td>1</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>10</td>
</tr>
<tr>
<td>Sprinklers/pipe</td>
<td>4</td>
<td>1</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>1</td>
<td>25</td>
</tr>
<tr>
<td>Struct damage</td>
<td>2</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>1</td>
<td>25</td>
</tr>
<tr>
<td>Vandalism/arson</td>
<td>1</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>Vandalism/Roof</td>
<td>1</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>7</td>
</tr>
</tbody>
</table>

Notes:

- High Impact: 5 - 1
- Low Impact: 1 - 5
- Weak Resources: 5 - 1
- Strong Resources: 1 - 5
Step 2: Begin The Business Continuity Plan

- What is the business continuity plan?
- Teams identified processes that were (and weren't!) critical to perform during an event.
  - We have to register students, decide their residency, evaluate athletic eligibility, schedule classrooms, graduate students, etc.
  - We will defer for a period of time (the most difficult list of all!):
    - Meetings
    - System testing
    - Data reports produced for campus departments.
    - Document imaging.
    - Training
Identify The Critical Functions of The Organization

- What are our services that are critical to continue to serve the mission of teaching, research and community service? To help identify these:
  - Would the failure to perform these functions result in irrevocable disruption to the student’s education (inability to register/drop/add; inability to award financial aid)?
  - Could it result in the irrecoverable loss of operational data (the timely entry of data)?
  - Could it result in significant financial loss to the institution (outside of the obvious loss of the disaster, the inability to admit students)?
  - Team leads worked within their units to determine:
    - Critical, recommended and non-essential activities.
Continuity Plans Developed

See examples:

- Assigning Classrooms to Classes
- Tuition Classification – Processing In-State Petitions
- We keep this information in the “Emergency Management Section” of our “Wiki”:
FORMS

As part of the business continuity plan, all emergency team leads posted ALL THEIR FORMS and BUSINESS PROCESSES in the “Wiki” so we could quickly reproduce these.
COURSE PROPOSAL FORM

Office of the Registrar
UNIVERSITY OF COLORADO BOULDER

COURSE PROPOSAL FORM

Complete this form for courses new to the ISIS Course Catalog (use the Course Revision Form for changes to existing courses).

Initially to be offered Catalog Year (a Catalog Year begins in a Fall Term and ends in a Summer Term and consists of Fall, Spring, and Summer Terms):

- Academic Group (College, School, or Program): ________________
- Subject Area (Dept., Course Prefix): ________________
- Catalog (course) Number: ________________
- Cross Listing Subject Area: ________________ Catalog (course) Number: ________________

1. Short Course Title (prints on Transcripts, Study Lists, and Schedule of Classes; cannot exceed 29 characters):

2. Long Course Title (prints in Catalog, cannot exceed 60 characters):...
Step 3: What would a “Post-Evacuation Site” Look Like?

• Personnel – who/how many would be required to accomplish the task (think staff and student employees)?
• Personnel – where could they work? Must they be on-site (front-line staff, management) vs. work from home (some IT staff, degree audit, ISIS development, etc.)?
• Work area – how much space is needed in our new site? What type of space is needed (secured?)
• Equipment and supplies – Computers? Printers? Telephone? Red pens?
• What services are needed – Mail delivery? Transportation Services? Warehouse? Specific power requirements? Access to non-central systems, like residency database? What needs to be secured at night?
• This all is added to the “post-evacuation site” map.
Step 4: Test The Plans

- Model the situation – you show up to work at Regent and it is no longer there.
- You begin to work at our back-up location:
- Do you have adequate space for each of your scenarios?
- Do you have adequate materials and supplies for your scenarios? Do you need forms, reports, etc.? If you need these, are these in your business continuity plan?
- Have you identified the equipment you need to do each task in your business continuity plan?
- Identify any shortfalls.
Step 5: Business Recovery Plan

- An event requiring activation of a business recovery plan will have been destructive and disruptive to the work place. The business recovery plan should address actions to support employee and employee problems, stress debriefings and employee assistance, along with cost recovery, insurance and mitigation issues.
  - 1. Identify a Salvage Team from your staff – who will go in and recover any usable assets (furniture, computers, reports, etc.)
  - 2. Identify a Service Restoration Team from your staff –
    - Implement standing contracts for facility clean up and repair
    - Work with institution facilities to establish utilities, data communications and communications in new site.
    - Establish supply delivery to the new site.
    - Determine what is needed for security at the new site.
Teams

• Emergency Planning Team – one member from each of the major units in the office. For CU Boulder, this was the registrar, and representative from IT, Degree Audit, Enrollment Services Unit, ISIS Development, FAST (Faculty and Staff Services)
• Salvage Team – members of the Emergency Planning Team
• Service Restoration Team – members of the Manager’s PLUS team –
  • Registrar
  • Senior Associate Registrar
  • 3 Associate Registrars
  • 4 Assistant Registrars
  • Communications Coordinator
  • ESR Manager
what we Also Have:

• Created “The Red Notebook”:
  • Evacuation Plans (don’t pick it outside of the campus bakery)
  • Evacuation Tips
  • Evacuation Lists – Immediate, 2-hour and 24-hour
    • Contact List – office and home/cell
"The Red Notebook"

- Evacuation Maps are noted on the front (exit from our office) and back (primary meeting location).
- Evacuation Tips are included.
  - "Buddy" – Additional help for some in the office with physical concerns.
  - "Sweepers" – vault, Call Center, downstairs and upstairs offices.
- Evacuation lists – immediate, 2-hour and 24-hour
And we Also:

- “Pocket sized” phone numbers and URL’s
- Have developed a “tornado or high wind” evacuation plan and tips for surviving a fire.
- Performed numerous training evacuation drills (and two “real life” – one for smoke, one for a “tornado”).
  - Be sure to tell other building occupants when you have a drill.
  - Take a “roll call” list to determine who didn’t make it to the primary site. Remember to remind your student employees.
- Worked with University of Colorado Police Department on “Active Shooter” training.
  - Installed “peep holes” in doors.
  - Established a “panic alarm” at our reception desks.
  - Reviewed what on our desks could be used as “weapons” if needed and escape routes (might be an office with a solid door – place the table in front – don’t huddle.
- Lanyards (ID, break-away, access)
And...

- Emergency Management plan with your IT shops is a beast of its own we have not done in years.
  - Need to determine your critical system processes.
  - Need to determine impacts:
    - Less than 24 hours down.
    - 1 – 3 days down
    - 4 – 6 days down
    - 7 days or over
- Apply costs to this – the faster the recovery and the more redundancy, it will cost that much more!
Questions?