Disaster Recovery and Business Continuity Planning Workshop

Jane Drews
University IT Security Officer
June 30, 2009
Learning Objectives

1. Identify the components of effective Disaster Recovery & Business Continuity Plans
2. Learn about resources which are available
3. Understand your unit’s responsibility for planning
4. Utilize tool to assist in development of a DR/BC plan
Outline

- Overview
- Department Information
  - Exercise 1
- Critical Functions
  - Exercise 2
- Information Technology
  - Exercise 3
- Key Resources
  - Exercise 4
Credit goes to “UC Ready” Tool!

Much of the content for development of the “DRBC-Planner” tool comes from the UC-Ready web tool developed at Berkeley

- ITSO and UIRM will investigate possibility of adopting UC-Ready web tool for use at the UI
- Should we adopt, information collected and input by you should be relatively simple to migrate
- We will keep you informed
Section 1: Overview
Overview

• **Disaster Recovery vs. Business Continuity**
  ▫ As duration of disaster increases, BC more important
  ▫ As scope of disaster increases, BC more important

• **Assessment of Risk:**
  No plan = accept full risk and consequence of a disaster
  Plan = identify worst case scenarios and mitigations to lessen disaster consequence and minimize loss
Overview

• Plans should address these aspects
  ▫ Physical
  ▫ Environmental
  ▫ Operational
  ▫ Personnel

• Critical functions or important?
  ▫ Not practical to cover everything in detail

• Consider “Natural” as well as “Artificial” Threats
  ▫ Planning process and outcomes
  ▫ Prevention measures
DR Fundamentals: Prevention and Mitigation

- Back-up methodology, off-site storage
- Physical security for equipment
- Logical security measures
- Administration and inventories
- Testing and training
University Responsibility

• Top level chain of command is already documented (CIMP)
• Communications regarding events
  ▫ [http://www.uiowa.edu/~pubsfty/cimp.pdf](http://www.uiowa.edu/~pubsfty/cimp.pdf)

• Infrastructure services:
  ▫ Network (ITS)
  ▫ Power and HVAC (FM)
  ▫ Physical space (FM)
  ▫ Telephone (ITS)
Things to Consider

- Personnel issues
- Payroll issues
- Purchasing

- Emergency Contacts
- Social distancing & working from home
Unit Responsibility

- Business Impact Analysis
  - Critical functions (prioritization)
  - Cost of failures
- Resources – people, systems, supplies, etc
- Vital records
- Recovery procedures
- Communications within unit
- Chain of command for decision making
Things to Consider

1. Disasters (obviously!) happen
2. Planning > Plan
3. Learn from experience and be better prepared
   - Crisis is not the time to deliberate decisions
   - Communication is a priority
4. You *will not* leave today with a finished plan
Section 2: Department Information
General Department Information

- Name, type of dept
- Personnel (categories, estimated numbers)
- Location(s) occupied
- References to other plans/documents
  - Pandemic plan
  - Evacuation/emergency plan
  - Faculty plan (teaching and research)
ABOUT ACTION ITEMS

• Most important part of the DR/BC Plan
  “What can your unit do to be better prepared?”
• Ideas, not commitments
• “Cost” estimates:
  ▫ Low (less than $1,000)
  ▫ Moderate ($1,000 to $10,000)
  ▫ High ($10,000 to $100,000)
• “Cost is” means one time, annual, or both
Exercise 1: Dept Information

- Navigate to: http://cio.uiowa.edu/itsecurity/resources/drbcp.shtml
- Save the spreadsheet to your desktop (“often”)
- Open and complete the Dept Info tab information as well as you can
- Utilize the Action Items tab. If there is information you need to collect (not available via web) – note it in your action items!
- Be sure to hover to see the Comments
Section 3: Critical Functions
Critical Functions

- **List of functions performed by your unit**
  - Don’t reinvent the wheel: “Essential Functions” for your unit were already identified in pandemic plans

- **Indication of function relative criticality:**

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical 1</td>
<td>Essential, must continue at normal and perhaps increased function</td>
</tr>
<tr>
<td>Critical 2</td>
<td>Essential, serious consequences if disrupted, must continue function at normal or reduced level</td>
</tr>
<tr>
<td>Critical 3</td>
<td>May pause briefly, but must resume function within 30 days</td>
</tr>
<tr>
<td>Deferrable</td>
<td>May pause if necessary, but should resume function as soon as conditions permit</td>
</tr>
</tbody>
</table>
Critical Functions - Examples

- Classroom instruction
- Laboratory research
- Process applicants (admission, degree, etc)
- In-patient, out-patient care
- Scheduling (courses, classrooms, etc)
- Produce Payroll
- Deliver supplies
Critical Functions - The Details

• Peak periods (i.e., start/end of sessions, FY)
• References to documents
• Dependencies to consider
  ▫ Upstream: HR, Registrar, ITS, FM, Purchasing, ...
  ▫ Downstream: may be groups or units
• Consequences of failure/reduction
• Coping strategies
Exercise 2: Critical Functions

- Complete the Critical Functions List tab first. Use pandemic plans to get started. 
  http://provost.uiowa.edu/docs/reports/PanFluResponsePlan.pdf
- Each critical function should be detailed in a separate (Critical Functions(1), etc) tab. To add more tabs:
  - Right click tab, select move or copy, click “X” to copy
  - Right click new tab, and move it before the “IT” tab
- Record actions to complete at the bottom of each tab
Section 4: Information Technology
Information Technology

- IT typically supports the unit’s critical functions
  - web site = communication vehicle
  - server = file storage, sharing, archive
- IT is centrally-supported as well as locally supported – they will be addressed separately
- Focus is on applications, inventory, procedures
- IT planning is to lessen impact on critical functions
  - Redundancy
  - Recovery procedures
  - Alternatives
Information Technology

• Recovery procedures should be documented, referenced, but *not* maintained within this tool
• Maintain and share relevant information
  ▫ Hardware
  ▫ Software (and appropriate licenses, access keys)
  ▫ Personnel (and appropriate expertise)
  ▫ Contact information – vendors, suppliers
• Redundancy, resiliency, recoverability, ....
Exercise 3: Information Technology

• Complete the IT tab as best you can
• First priority is support of critical functions, but everything should be collected
  ▫ Central “Enterprise” applications utilized
  ▫ Department applications
  ▫ Servers – describe those owned and managed by your unit
  ▫ Workstations – what inventory do you have, and how many, in general terms
  ▫ Backups – looking for adequacy, not details
• Review the IT-Recovery tab scenarios and make notes
Section 5: Key Resources
Key Resources - Personnel

• General things to consider before emergency
• Key personnel
  ▫ Start with information from pandemic plan
• Working from home
  ▫ Survey your department personnel?
  ▫ Requirements to make this successful?
• Other personnel considerations
  ▫ Teams, skills, functions, replacements, alternatives, etc
Key Resources - Non Personnel

- Documents – where are primary/definitive?
- Equipment and supplies
  - Office equipment
  - Other equipment
  - Supplies
- Facilities and transportation
  - Space
  - Utilities
  - Transportation
- Other resources
Exercise 4: Key Resources

• Complete the **Key Resources-Personnel** tab
  ▫ Chain of command and decision makers
  ▫ Expertise should be considered
  ▫ Consider strategies to collaborate
  ▫ Consider the support of critical functions

• Complete the **Key Resources-NonPersonnel** tab
  ▫ Can’t prepare meals without food
  ▫ Can’t run busses without gas
  ▫ Can’t treat (some) illness without drugs
Next Steps

• Save the plan!
• Review your recorded actions
• Complete the missing parts of your plan
• Share within your department as draft
• Obtain executive review and acceptance
• Provide FEEDBACK on the tool

• “How to conduct a tabletop exercise” ????
Thank You