Business Continuity Planning & Low-Hazard Laboratories

or… How much of that elephant have you already eaten?

John J. Kelly, CIH
Risk & Emergency Manager
Jefferson Lab

Jefferson Lab
Thomas Jefferson National Accelerator Facility

What is Business Continuity Planning (BCP)?

Advance arrangements and procedures that enable an organization to respond to an event so that critical business functions continue within tolerable levels for the duration of interruption.

Blah, blah, blah!

If you can't do without something (info, equipment, workspace), you need…

- ⇨ Redundancy
- ⇨ Protection in depth — maybe both
- ⇨ Relocation site (selected in advance, with equivalent security)
- ⇨ Quick access to resources
- ⇨ A plan on how all of this works

BCP sits at an intersection of Emergency Management and Risk Management.

- Business Continuity Planning should be driven by risk:

  Likelihood of an undesirable event × severity of the outcome(s)

- Not all site emergencies necessarily pose threat to business continuity.

*BCP is Precursor to **Disaster Recovery***

- A plan, activities, and resources designed to return the facilities to acceptable operational condition for resumption of organization's critical business functions.
- Tends to be more concerned with restoration of facilities, utilities, other “hard targets.”
- More exciting than BCP, therefore a potential distraction.

- Overall, the private sector has more robust BCP than do government agencies & government-funded enterprises.
- If traditional self-interest wasn't a sufficient motivator…
  - 9-11 was an "epiphany" for business and insurance communities.
  - *Sarbanes-Oxley Act of 2002*
    - Most far-reaching regulatory changes affecting public companies since the 1930's
    - Management certifications of financial statements
    - Management assertion about internal controls
    - ***Greater disclosures about risks and related controls***

So, look to the private sector as a model?

Well, maybe.

Competition, customer & stockholder expectations, lenders & insurance requirements all tend to drive BCP. You'd think they'd all be on top of this since owner/shareholder investment is at risk.

But…

According to the Department of Labor…

43 percent of businesses experiencing a disaster never reopen.

29 percent of those that do reopen close within two years.

Consider this…

- ⇨ Character of science, R&D facilities are a bit like entrepreneurial businesses…
  - Influenced by personality/style of principal/CEO/director
  - Many key decisions are made only at the top
  - Succession planning is anathema
  - Have narrow “customer” base
- ⇨ Not uncommon that BCP gets short-shrift relative to protecting expensive assets/apparatus and the production/research agenda.

Some nuances for DOE labs:

- Can’t buy our way of a disaster
- Unique apparatus
- No insurance for federal property
- Other considerations may be may be driving the Emergency Management train – possibly to the detriment of BCP. For example:
  - Scientific program
  - Community relations
  - Hazmat & radiological aspects
  - Security

Distinctions between BCP at low-hazard labs vs. others?

- Drills & exercises are easier to conduct within non-classified buildings.
- Security aspects less likely to dominate exercises.
- Less disparity between site “worst-case” event and the un-dramatic, but highly disruptive loss of business infrastructure and capabilities.

Elements of a Basic Business Recovery Plan:

- Maintain communication with employees
- Maintain communication with key business and off-site resources
- Vital records -- storage and retrieval
- Electronic data -- storage and retrieval
- Alternative work locations
- Restoration of (or alternative) computer hardware, network, and telecommunication equipment & systems
- Resumption of procurement and time-critical accounting systems
- Modify security procedures to safeguard “compromised” assets

All of these require advance planning, writing things down, getting informed input and buy-in, and some kind of periodic practice.

What are vital records?

Kind of like the term ***“essential personnel.”***

It depends on whom you ask.

Records considered vital usually meet one of three criteria:

1. Records essential to the continued functioning or reconstitution of an organization during and after an emergency.
2. Records required by law and regulation.
3. Records which protect the legal and financial rights of the government, the Contractor, and the individuals directly affected by lab activities.

Two methods of protecting vital records:

Dispersion

Sending copies of vital records to locations other than those where the originals are housed.

Duplication

The preparation of additional copies of a record. The process includes microfilm, scanning, optical or magnetic tape storage, photocopying, etc.

One of the best strategies for quick recovery of vital records is to discard promptly the non-essential.

Information Technology is on par with Vital Records as the greatest concern in BCP.

Information Technology's Role:

- ➩ Should not be responsible for creating individual department plans
- ➩ Leadership in plan development.
- ➩ Generally has the best appreciation and understanding of information flow throughout the organization.
- ➩ Often in the best position to identify and assess the following areas.
    - Interdepartmental Dependencies
    - External Dependencies
    - Internal and External Exposures

IT is notoriously reluctant to accept NIH strategies offered by EM or RM.

BCP planning may benefit by separate risk assessment of scientific and business computing resources.

A few, high-leverage tips for business continuity planning:

- Fix the big holes first.
- Effort required for 100% perfection = 10 × (effort for 95% perfect)
- Seize every opportunity to build-in BC features when new stuff is being designed (be a benevolent parasite!)
- Pre-arrangements for emergency purchasing
- Remote connectivity for essential business functions
- Ability to write checks in a different location, on different equipment: payroll, accounts payable

Recovery success relies on clear, pre-identified authority. *Not a time for collective decision-making (that ought to have happened in planning and refinement)*

- Don't overlook employee welfare in disaster planning and recovery.
- Nuts-and-bolts portion of BCP should fit in a pocket or glove compartment.
- Focus on developing strategies rather than procedures.
- When in doubt, keep it simple.
- Process diagrams or flow charts are useful "diagnostic" tools. They may even be best way to document procedures.
- Plan for worst- case scenarios; reality is often short of that.
- Everyone who has a defined role in EM needs to be recognized via performance appraisal.
- Keep perspective. Emergency Preparedness is about:

  Life Safety - FIRST

  Business Continuity - Second

  Asset Recovery - Third
- Potent temptation to fixate on process. Best antidote is to use exercises to demonstrate desired outcomes

Testing your Business Continuity Plan

- ***It is impossible that testing a plan can result in a failure***. If it works, good; if it doesn't work, good to know that too.
- Integrate BCP into tests, drills, exercises for regular operations.

  e.g. Aspect of a structure fire or major storm damage
- Exercises should be clearly value-added, and a good use of everyone’s time.
- Find and use good facilitators and evaluators: observant with no axe to grind. (If you have access to insurance industry consultants, they can be a good, impartial contributor.)

Information Resources you may find useful:

The Business Continuity Planners Association (BCPA)
http://www.bcpa.org/metadot/index.pl

“Disaster Recovery Journal”
http://www.drj.com/

INFOSYSSEC - The Security Portal for Information System Security Professionals
http://www.infosyssec.org/infosyssec/buscon1.htm

Dictionary -CONTINUITY OF OPERATIONS PLAN (COOP)
http://www.drj.com/glossary/drjglossary.html

“Eating An Elephant”
http://www.operationalrisk.info/bc002.html

Shelter in Place
http://www.tallytown.com/redcross/library/ShelterInPlaceAtYourOffice.pdf

Emergency Planning Considerations for the Disabled
http://www.nod.org/pdffiles/epi2002.pdf

Resource Topics: Weather and Natural Disasters
http://www.sb.thehartford.com/reduce_risk/loss_library/Weather_Related_Natural_Disasters/

“Report of Presidential Ad Hoc Committee for Building Health and Safety under Extraordinary Incidents”
http://xp20.ashrae.org/ABOUT/Summary.pdf

Pamphlet: “Open For Business”
http://www.ibhs.org/docs/openforbusiness.pdf

“Getting Back to Business”
http://www.ibhs.org/docs/GBB.pdf

Federal Facilities Council -- Business Continuity and Disaster Recovery Planning References
http://www7.nationalacademies.org/ffc/Business_Continuity_Emergency_Preparedness_Resources.html

North Carolina State University, Business Continuity and Disaster Recovery Department
http://www.ncsu.edu/ehs/BCP/add_ref/campus_presentations.php

“A PRACTICAL GUIDE FOR UNIVERSITY CRISIS RESPONSE”
http://www.crisisinfo.org/universitycrisisresponse/documents.htm

Argonne National Laboratory's Emergency Preparedness Group
http://www.dis.anl.gov/ep/ep_home.html

Emergency Preparedness - Business Continuity for Facilities Management
http://www7.nationalacademies.org/ffc/jay.PDF

Jefferson Lab Emergency Management Web Page
http://www.jlab.org/intralab/emergency/

A professional certification organization:

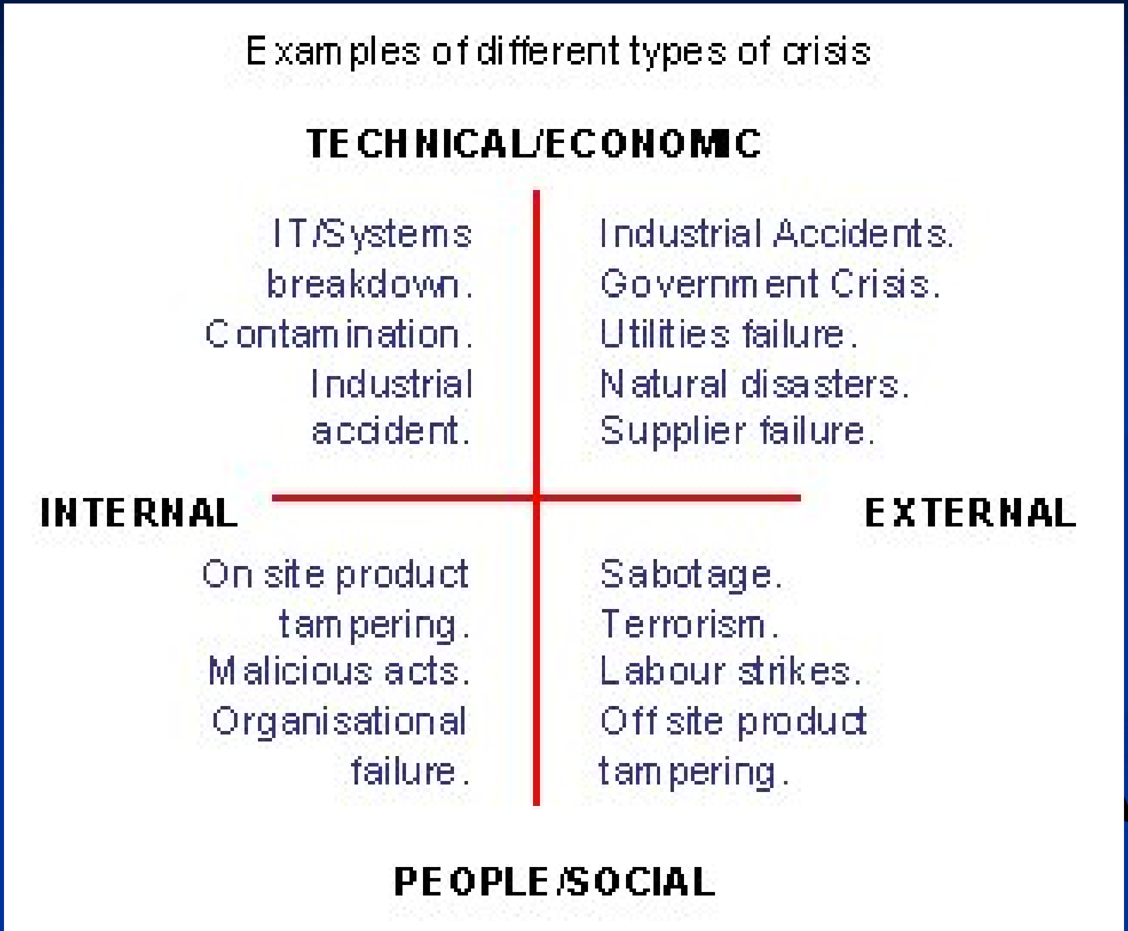
DRI International
201 Park Washington Court
Falls Church, VA 22046-4513
Phone: 703-538-1792 Fax: 703-241-5603
http://www.drii.org/

“**DRI International** was founded in 1988 to provide a base of common knowledge in contingency planning, a rapidly growing industry. DRII also administers the industry's premier global certification program for qualified business continuity and disaster recovery planners.

“**The Professional Practices for Business Continuity Planners**, our common base of knowledge, serves as the industry's best practices standard.

“And, our **highly acclaimed training courses** continue to educate and inform business continuity and disaster recovery planners worldwide.”

JK Disclaimer: I have no information about this organization other than what appears on their website.



Examples of different types of crisis

TECHNICAL/ECONOMIC

IT/Systems breakdown.
Contamination.
Industrial accident.

Industrial Accidents.
Government Crisis.
Utilities failure.
Natural disasters.
Supplier failure.

INTERNAL

EXTERNAL

On site product tampering.
Malicious acts.
Organisational failure.

Sabotage.
Terrorism.
Labour strikes.
Off site product tampering.

PEOPLE/SOCIAL

Source:
http://www.dti.gov.uk/mbp/bpgt/m9ba91001/m9ba910013.html#toc_5

The problem is that even in best-of-class IT shops, an estimated 20% of all backups fail to fully recover. When servers move outside of class-A data centers, such as remote or branch offices, departmental servers, mid-market enterprises or small businesses, these failure rates escalate to 50%.

'It's the restore, stupid!' Advice by Bob Cramer
APRIL 23, 2003 (COMPUTERWORLD)