

How to Develop and Conduct
a Successful BCP/DRP Exercise
. . . Or . . .
READY, SET, EXERCISE!

DRJ Fall 2009 Workshop by:

Steven Goldman, Ed. D.

Speaker and Consultant

CrisisPlan@aol.com

(978) 256-2332

Agenda

- ✓ Introduction
- ✓ Why Exercises are Important to Your BCP/DRP Program
- ✓ Drill / Exercise Development Steps
- ✓ Scope and Objectives
- ✓ The Scenario Development Team
- ✓ Scenario Ideas you can use
- ✓ Sequence of Events (Time Line)
- ✓ Making it Real . . .
- ✓ Conducting the Exercise
- ✓ The Critique
- ✓ Develop a Timeline! (*if time permits*)
- ✓ Summary

. . . and Also . . .

- **Fire Exits**
- **Cell Phones and Pagers – OFF or VIBRATE!**
- **Questions Anytime**
- **Rants and Raves**
- **Adapt this workshop to *your* specific needs/organization.**
- **DRJ Evaluation Forms – Please complete!**
- **There will be a Quiz!**

Why Exercises are Important

I Hear ⇒ I Forget

I See ⇒ I Remember

I Do ⇒ I Understand

-Chinese Proverb

Training, Drills, and Exercises

- **Classroom Training / Orientation**
- **Individual Skills Training**
- **Team (or department) Drill**

- **Tabletop Drill**
- **Company-only / Functional Exercise**
- **Full-Scale Exercise**

Tabletop drill vs. Full-scale Exercise

Trait	Tabletop Drill	Full-scale Exercise
Scope	Internal only	Internal and external
Development time	1 – 2 months	Up to a year
Simulation	Much	Minimal
Events Time	Relative	Realistic
Locations	Usually one	Several / all
Facilities	Actual or simulated	Actual use
Equipment	None / some	Actual use
Responders	Key / many	Most / all
Stress on responders	Eventually	Yes!
Stated agenda	Training; find problems	Response; fix problems
Hidden agenda	Shed light; get support	Darwinism

Benefits of a Successful Drill/Exercise

For your Responders:

- Training; understanding of BCP/DRP; the “AHA!” moments
- Paper/electronic plans; tools ⇨ People responding
- Responders see the effects of their actions and decisions
- Participants can “win” with proper corrective actions

For your Program:

- Identifies weaknesses, gaps, and areas for improvement before a crisis
- Validates your BCP / CM / DRP plan and program
- Trains responders; improves their competence; inspires their confidence; builds teamwork within your organization
- If done well: Excellent recognition, visibility, trust, and respect for your program and for you

Steve’s Exercise Planning Checklist

- Define
- Develop
- Set up
- Conduct
- Follow up

Steve's Exercise Planning Checklist: Define the Exercise

TASK	T- Date
Start: determine you need to conduct an exercise. Determine approximate scope. Obtain your management and senior management support (<i>Necessary throughout planning!</i>)	-9 to -12 months
As necessary, preemptively reserve company and hot site facilities and services	-9 to -12 months
Decide what you need to evaluate/test (Use your Three Year Plan)	-6 to -12 months
Define the scope and establish the objectives for the Exercise	
Identify limitations to Exercise conduct	
Revise objectives accordingly; finalize exercise scope, objectives, and limitations	-6 to -9 months
Determine participants (internal and external), needs, and schedule/dates.	-6 to -9 months
Obtain buy-in and permissions; secure people (scenario developers, participants, executives, external); secure/reserve facilities, food, logistics, paperwork	- 6 to -8 months
Develop and publish the Exercise Schedule	-6 months
Assemble the Scenario Development Team; start scenario development meetings	-6 months

DRJ: Fall 2009

© Steven B. Goldman

9

Steve's Exercise Planning Checklist: Develop the Exercise

TASK	T- Date
Hold scenario development/review meetings	Biweekly/as needed
Verify security control of the scenario events	Throughout
Develop the scenario sequence of events	Start at -6 months; complete at -2 weeks
Determine limits of participant response to each action	
Develop messages, mini scenarios, data	
Clarify/Coordinate efforts of internal and external response organizations	
Determine requisite mock-ups, props, diagrams, pictures, images	
Secure any additional logistics support (<i>People, facilities, food, paperwork</i>)	
Revise the above as necessary; do not lose sight of the scope and objectives!	
Complete the Exercise manual	-4 to -8 weeks
Select the Exercise controllers/evaluators; develop their tools	
Set up the Exercise control cell; develop the draft Exercise Communications List	

DRJ: Fall 2009

© Steven B. Goldman

10

Steve's Exercise Planning Checklist:
Set up / Conduct / Follow up

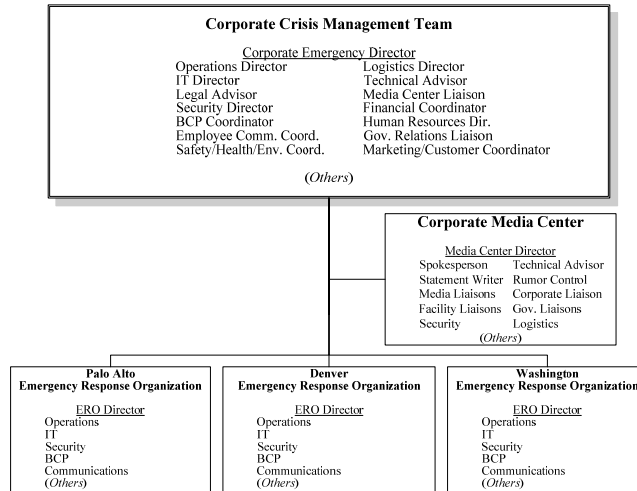
TASK		T- Date
Set up	Complete the mock-ups, props, diagrams, pictures, images	-7 days
	Finalize participants, control cell, and exercise communications lists	-5 days
	Finalize the Exercise manual; reproduce copies as needed	-5 days
	Develop controller, evaluator, control cell, and responder briefing materials	-3 days
	Inform employees, the public, and the media (as needed) of the Exercise	-2 days
	Brief participants (internal and external) on scope, limits, and logistics of the Exercise	-1 day
	Conduct controller/evaluator and control cell training; incorporate last-minute revisions	-1 day
Conduct	CONDUCT THE EXERCISE	0
Follow up	Conduct a formal Exercise critique; provide for responder feedback	+1 day
	Evaluate/document the Exercise; send out the draft Exercise Report and Action Plan for review	+7 days
	Submit Final Exercise Report and Action Plan	+14 days
	Revise plans, procedures, contacts, facilities, equipment, and training based upon Exercise lessons learned and Action Plan.	+30 days

The ACME Corporation

Corporate Organization

- Corporate Headquarters Boston, MA
- R&D Division Palo Alto, CA
- Manufacturing Division Denver, CO
- Financial Services Division Washington, DC

The ACME Corporation Crisis Management Organization



Exercise Manual: Contents

1. Scope and Objectives
2. Exercise Information
3. Participant Information and Assignments
4. Schedule
5. Exercise Scenario and Messages
6. Mini-Scenarios
7. Crisis Communications Messages
8. Simulated External Responses
9. Appendices
10. Critique (*Insert after Exercise*)

Tabletop Drill Manual: Contents

- 1. Drill Information / Briefing Materials**
- 2. Drill Timeline / Sequence of Events / Messages**
- 3. Other Information / Data (if any)**

The Three-Year Exercise Plan

- **Annual Objectives**
 - Activate and operate CCMT, CMC; fully coordinate with one division; etc.
- **New Objectives** (*determined each year*)
 - Test new notification system; demonstrate podcasting; etc.
- **Year 1 Objectives**
 - Palo Alto Division to participate with CCMT; demonstrate full shift turnover; etc.
- **Year 2 Objectives**
 - Denver Division to participate with CCMT; after hours start; loss of network; etc.
- **Year 3 Objectives**
 - Washington Division to participate with CCMT; full hot site use; etc.

What are Your Limits?

- Operations
- Personnel
- Resources
- Internal Support
- External Organizations
- Funds
- Imagination!

Example Scope Elements - 1

The Exercise will test the major response capabilities of:

- The Corporate Crisis Management Organization
- The Corporate Media Center Organization
- The Denver Emergency Response Organization

Corporate

- The ACME Corporate Crisis Management Team and the Media Center will be fully activated and operated.
- The Exercise will be held during the work day; it will be conducted between 0800 and 1600 hours. Activation will be on a real-time basis.
- The IT Disaster Recovery Plan will be activated and implemented within ACME Corporate. Communications to and activation of the Hot Site will be required, but transfer of operations will not be exercised.
- The following departments will participate: *{list}* and the following will be simulated: *{list}*.
- *(Others as appropriate)*

Example Scope Elements - 2

Denver Division

- The Denver Manufacturing Facility Emergency Response Organization will fully activate and respond on a real-time basis.
- County and city emergency responders will participate. The exercise will require the mobilization of their resources, including the Denver Fire Department
- Continuity/Recovery of at least one department, including simulated relocation
- State and Federal agencies will not participate; their response will be simulated.
- The following departments will participate: *{list}* and the following will be simulated: *{list}*.
- *(Others as appropriate)*

Palo Alto and Washington Divisions

- The Palo Alto and the Washington Divisions will not participate in this exercise.
- The Palo Alto and the Washington Divisions will provide telephone controllers to simulate their response to requests for information and/or action

Exercise Objectives

- If your exercise is considered a _____
- Then your exercise objectives are your _____
- However, you also need to know _____!

Use SMART Exercise Objectives

- **S**imple (Specific and Concise)
- **M**easurable (Quantifiable)
- **A**chievable (Real-time or with planning)
- **R**elevant (Challenging and realistic)
- **T**rackable (Relative to a procedural step)

Sample Objectives - 1

CRISIS MANAGEMENT TEAM

1. Demonstrate the capability of the Corporate Crisis Management Team to mobilize in a timely manner on a real-time basis.

How Satisfied: *In accordance with Crisis Procedure 1.2, the Crisis Management Team (CMT) should be pronounced operational within 30 minutes of the crisis declaration.*

NOTIFICATION METHODS AND PROCEDURES

1. Demonstrate the ability of CMT personnel to send initial emergency notification messages to the Financial Community. **LIMITATION:** Financial agencies will be simulated.

How Satisfied: *In accordance with Crisis Procedure 3.7, the CMT Financial Coordinator should notify the following financial institutions within 30 minutes of the CMT being declared operational: {...list...}*

2. Demonstrate the capability for ACME personnel to forward incoming phone calls to the Media Center when questioned about the emergency.

How Satisfied: _____

Sample Objectives - 2

MEDIA AND PUBLIC RESPONSE

1. Demonstrate the capability of the Media Center to formulate accurate, clear, and understandable messages for the media and public.

How Satisfied: _____

2. Demonstrate the ability to monitor the Media to detect and correct errors.

How Satisfied: *Messages with erroneous information will be injected at 1025, 1130, 1240, and 1305. The Media Center Staff should recognize the errors and correct them in accordance with Media Center Procedure 4.7.*

MAINTENANCE OF MARKET SHARE

1. Demonstrate the Marketing Department's ability to develop a strategy and timetable to regain Widget market share.

How Satisfied: *Messages will be injected describing ACME's loss of market share. The Marketing Department should assess the situation and develop pertinent strategies. NOTE: This action will be prompted if appropriate Marketing Department activities do not occur by 1200.*

Sample Objectives - 3

IT

1. Demonstrate the ability to assess, isolate, and repair the loss of network communications to/from the Denver Division.

How Satisfied: *Successful completion of Mini-scenario #12. A server problem will be injected at 1010. IT personnel should take appropriate action to assess and restore network communications to/from the Denver Division.*

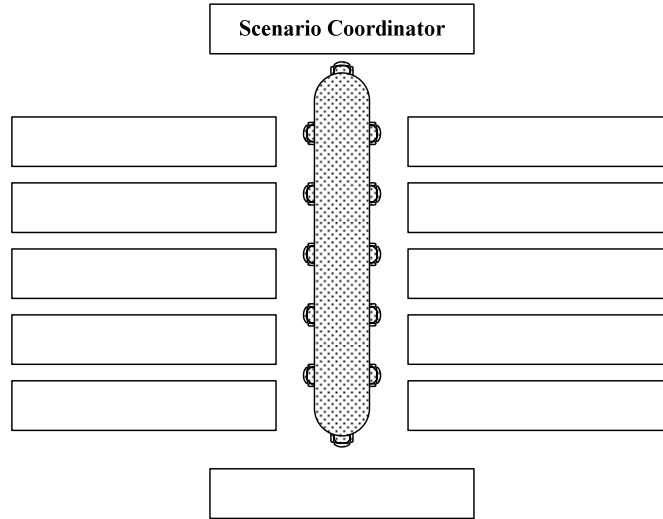
2. Demonstrate the ability to activate the Hot Site.

How Satisfied: *A problem in the computer network (Mini-scenario #14) will require activation of the Hot Site. DRP Procedures will be implemented up to but not including Section 10.8 "Transfer of operations." Limitation: IT personnel will make arrangements per procedures, but will not travel beyond the Corporate Office. Actual transfer of IT operations will not be exercised. The IT DRP Team will be pre-staged in the Hot Site.*

3. Demonstrate the ability to recover critical business applications after a postulated network failure.

How Satisfied: *The IT DRP Team (pre-staged in the Hot Site) will recover the following critical business applications {list} within the RTO's promulgated in the DRP and BIA {list}.*

The Scenario Development Team



Scenario Ideas

- 1. IT Problems**
- 2. Natural Disasters**
- 3. Business Crises**
- 4. External Threats**
- 5. Location Threats**
- 6. Terrorism Threats**
- 7. Anticipatory Events**
- 8. Specific Company/Agency Threats**

Scenario Ideas: Class Activity

Assigned Crisis Type (e.g., Natural Disaster): _____
1. (e.g., Hurricane)
2.
3.
4.
5.
6.
7.
8.
9.
10.

Other Sources of Inspiration!

- Business Impact Analysis (BIA)
- Terrorism Impact Analysis (TIA)
- Environmental Impact Statement (EIS)
- Risk Manager or Lawyer

- Annual and 10(k) Reports
- Trade Magazines
- Newspapers/Internet
- Disaster Ideas by Walking Around

Keep a file of potential disasters you can use!

Sequence of Events – Denver Plant

Time	Key Event
8:00	Initial Conditions established; commence Exercise
8:05	In Denver Building 4, process heater HX-2A develops an oil leak. This causes a large fire.
8:07	Workers nearby hear several loud “pops”. An operator investigates.
8:09	The operator is overcome by fumes and collapses.
8:10	Fire alarms sound; the Fire Brigade is toned out.
8:15	The Denver County Fire Dept. arrives at the plant.
8:15	The Denver VP declares a plant emergency per Emergency Procedure 2.0. The ERO is activated.
8:45	A Channel 5 news team arrives at the plant gate.
9:00	The fire spreads to the warehouse. . . .

Sequence of Events - Corporate

Time	Key Event
8:00	Initial Conditions established; commence Exercise
8:15	The Denver VP notifies the Operations SVP about the plant emergency and its impact on production.
8:20	Per Corporate Crisis Procedure 1.2, the Corporate CMT and the Corporate Media Center are activated.
9:25	Boston Channel 7 is reporting a fire has killed several . . .
10:10	Server DEN1-CORP3 in the corporate data center fails, resulting in a loss of network communications to/from the Denver Division.
10:30	CNN reports that the ACME disaster will cause sales of Widgets to plummet. The reporter further states that ACME’s main competitor, the Pumpkin Corp., will soon become the sales leader in Widgets.
	<i>(Additional events)</i>

Initial Exercise Conditions

- **Nothing is happening:** Typical day - then a crisis hits!
 - Some people/equipment may be away/out of service
 - Crisis situation may start small and build
- **Stuff is happening:** Crisis occurred and is underway!
 - Data center on fire; hurricane or flu predicted; problem in remote office
 - Fire/police show up at scene; employees in parking lot
- **Stuff has happened:** Initiating event is over - now what?!
 - Data center fire is out; injuries at hospital; DR team at hotsite
 - Hurricane/earthquake damage reports in; buildings are cordoned off

Make it Real . . .

- ☞ Doctored photos or maps of “damage”
- ☞ Smoke-generating machines
- ☞ Colored water/sand to simulate spills
- ☞ Tape off “flooded” or inaccessible areas
- ☞ Moulage for simulating injuries; live “victims”

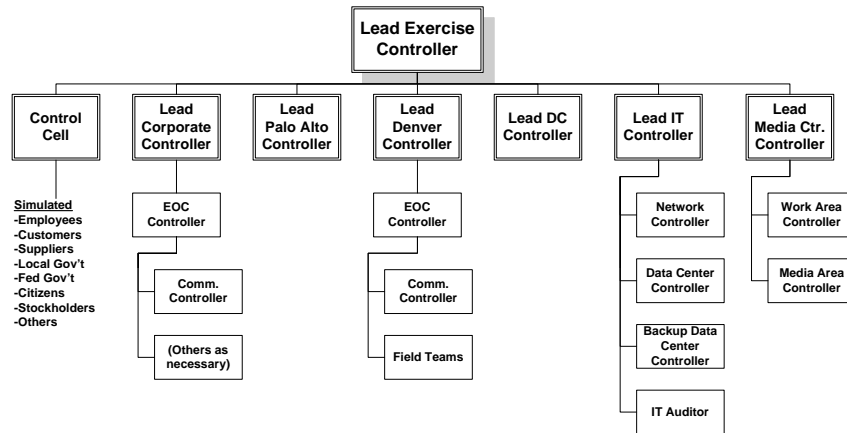
- ☞ Use real broken equipment for repair teams
- ☞ Disable actual systems
- ☞ Actual travel to the Hot Site; transfer IT operations

- ☞ Exercise messages, e-mails, articles, blogs, web pages
- ☞ Audio- and video-tapes of mock news reports
- ☞ Real Media/Journalism students at the Media Center

Exercise Organization

- Responders
- Controllers
- Evaluators
- Control Cell
- Observers

Full-Scale Exercise Control Organization

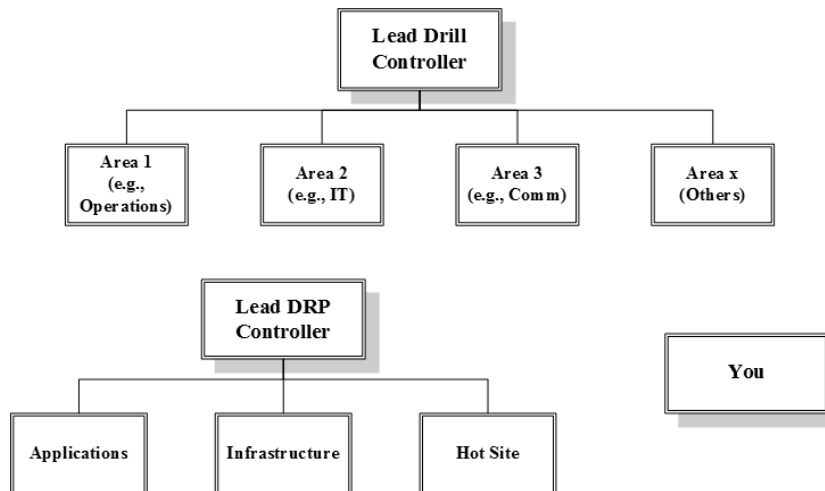


Exercise Control Organization

Controller	Evaluator	Control Cell
<ul style="list-style-type: none"> • Ensures Exercise proceeds as planned • Injects pre-scripted messages • Observes player response for free play to ensure Exercise is on course • Oversees free play by Control Cell • Coordinates with other Controllers • Ensures non-Exercise events do not interrupt response • Records player actions, successes, problems, areas for improvement • Conducts debriefing; gathers paperwork • Trained to the emergency plan, procedures, scenario, expected responses and accuracy of responses; familiar with exercise, objectives, message forms and message delivery 	<ul style="list-style-type: none"> • Independently observes Exercise • Reports compliance with plan, positives and negatives of response • Trained to the emergency plan, procedures, response organization • Familiar with evaluation criteria and evaluation forms • Should evaluate the exercise scenario too • NOTE: Sometimes the Evaluator role is combined with the Controller role. 	<ul style="list-style-type: none"> • One or several people in Control Cell room on telephones • Serves as "actors" to portray non-participating people/agencies; receive as well as make calls or internet inquiries • Can also act as news media, citizens, employees, etc. calling in • Each person in cell may assume multiple roles • Cell is physically isolated from response areas • Familiar with exercise, objectives, message forms and message delivery • Trained to the emergency plan, procedures, scenario, expected responses and accuracy of responses

Tabletop Drill Control Organization

Three Examples



The Critique

WHEN:

- Immediately after the Drill/Exercise, conduct an in-facility Critique.
- As soon as possible after the Drill/Exercise, conduct a Consolidated Critique. This can be right after the in-facility Critique or within a week.

HOW:

- Discuss Critique purpose, format, "rules", time available, etc.
- Briefly summarize objectives and scenario.
- Go around the room and get everyone's feedback: First Players, then Evaluators, finally you. Keep it moving! Do NOT solve problems!
- Summarize: "We met 18 of the 19 objectives... overall, things went very well...tough scenario..." Be honest; participants know how things went.
- Conclude with praise, encouragement, action plan, commitment, thanks.

POINTERS:

- Always: Good training / Learned much / Improve communications.
- Internally assess the criticisms: Some are valid; some are defensive.
- Keep an open mind: there may be more than one solution to a problem.
- Be honest; nothing personal; watch out for career suicide.
- Emphasize positives as well as "opportunities for improvement."

Develop a Timeline!

Using the
Sequence of Events Timeline grid format (on next slide):

Develop a (brief) Disaster Scenario for a Division

or

Develop a (brief) Crisis Scenario for Corporate

Develop a Timeline!

Company Name:	
Company Product/Service:	
Time	Key Event
8:00	Initial Conditions established; commence Exercise.
15:00	The Exercise is terminated; commence the critique.

Develop a Timeline!

How to get started:

- List the assumptions you want to make (do not get hung up on these!) :
 - Name of your Company
 - What your Company does/makes/provides

Consider these basic objectives:

- A disaster occurs that activates the Division Emergency Response Organization
- Later, a Corporate Crisis occurs, requiring the Corp. Crisis Management Team
- (*Optional*) It's going to be a bad day at the office: something else happens.

Hints:

- Work together, compromise, make it happen!
- Use the ACME Corporation as a model (or not)
- Use a scenario idea or two from before (or not)
- Do not solve problems now; that would come in the next revision
- Do not get bogged down in details; those are developed in the mini-scenarios
- Develop events and ramifications, not elaborate response actions.

Summary

Developing a successful Drill or Exercise requires:

- Hard (but Satisfying) Work
- 2-to-12 Months Lead Time
- Senior Management Support

- Desire to Really Test Your Program
- Attention to Detail
- Creativity, Foresight, Leadership

You can do it!

Thank you!

- **Questions? I will be here for a while.**

- **Please complete the DRJ Evaluation Forms.
Help is available!**

- **Feel free to e-mail or call Steve with questions,
comments, concerns, etc.**

CrisisPlan@aol.com

(978) 256-2332

Scenario Ideas:
IT Problems

- Computer Virus
- Fire / Explosion in Data Center
- Network / Servers Failure
- Support equip. failure (e.g., AC)
- Software error
- Power failure (Int. or External)
- Internet overload / slow / failure
- Hackers
- Other:
- Denial of service attack
- Hot site unavailable
- Off-limits data center building
- Programming error
- Rogue server
- Service Provider Failure
- Data Center flooded
- Other:

Scenario Ideas:
Natural Disasters

- Hurricane
- Tornado
- Earthquake
- Flood / Flash Flood
- Tsunami
- Pandemic
- Lightning Strike
- Fire
- Drought
- Other:
- Heavy Snowfall
- Ice or Ice Storms
- Landslides / Mudslides
- Dam Failure
- Infestation
- Contamination
- Sinkholes
- Extended Cold / Heat
- Solar Magnetic Storms
- **Moose**

Scenario Ideas:
Business Crises

- Product Problem / Recall
- Corporate Takeover
- Strike / Lockout / Labor Problem
- Workplace Violence
- Executive Death(s)
- Executive Dismissals / Raiding
- Private data lost / released / stolen
- Sexual / Racial Harassment
- Whistle Blowing
- Class Action Lawsuits
- Consumerism Actions
- Mismanagement
- Embezzlement
- Supplier Problem / Disaster
- Key Customers Loss
- Sex Scandal
- Media Scare (Real or Not)
- Unfavorable Court Ruling
- Major Promotional Error
- Other:

Scenario Ideas:
External Threats

- Terrorist Threat
- Bomb Threat
- Crisis at Neighbor
- Sabotage / Theft / Arson
- Legislation
- Another's Crisis on Your Property
- Crisis Thought to be Yours
- Supplier Loss
- Crisis in Same Industry
- Other:
- Government Restriction
- Limited or No Property Access
- Communication Failure
- Transportation Loss
- Rumors Being Spread
- Kidnapping
- Hostage Situation
- Political Situation
- Technology Progress

Scenario Ideas:
Location Threats

- Chemical Plant
- Nuclear Power Plant
- Ocean / River / Lake
- Flood Plain
- Airport
- Major Highway
- Major Railway
- Military Base
- Federal Building
- Other:
- Foreign Embassy
- Hazardous Neighbor
- High Target Neighbor
- Office above 10th Floor
- Cultural Clash
- War Imminent or Declared
- Special Events (e.g., DNC in Boston)
- Lack of Skilled Labor
- Dependency on one employer

Scenario Ideas:
Terrorism Threats

- Bomb Threat (Credible or not)
- Office building bombed
- Terrorism event nearby
- IED / RDD detonated
- No Access to your Building(s)
- Key Executive Kidnapped
- Hostage Situation (local / foreign)
- Key Customer Loss
- Key Supplier Loss
- Other:
- Internet Disruption
- Financial Disruption
- Call out of National Guard, etc.
- Transportation limitations: staff
- Transport limitations: product
- Guilt by association
- Confiscation of equipment / files
- Anthrax in mailroom
- Staff refusal to report to work

Scenario Ideas:
Anticipatory Events

- Executive Scandal
- Poor Earnings Expected
- Key Customer Loss
- Key Supplier Loss / Failure
- Hurricane Forecast
- Tsunami Warning
- Severe Weather Forecast
- Executive(s) Departure
- Executive(s) Resignation
- Senior Executive to Rehab
- Fraud Discovered
- Bankruptcy to be declared
- Power to be Shut Off
- Serious Product Problem Discovered
- New Computer Virus Unleashed
- Lawsuit to be Filed
- Rumors Being Circulated
- Guilt by Association
- Other:

Scenario Ideas:
Specific Company/Agency Threats

- Intellectual property stolen
- Huge loss of market share
- “Secret formula” on Internet
- Brand name trashed
- Competitor challenge
- Disease outbreak/shooting in college dormitory
- Other: