**Threats and Hazards: Event Challenges and Impacts**

***Event Disruptions Are Always A Possibility… Planning Is the Key to Surviving Them***

In the past several years, Americans have experienced unthinkable disasters resulting from terrorist activity. The September 11 attacks on the World Trade Center and the Pentagon struck on a peaceful, sunny morning with no warning. War with Iraq has made our country and our people more vulnerable to terrorist activity and, even with the war at an end, the Department of Homeland Security warns that terrorism remains a very real threat for the foreseeable future. The bombing of the federal building in Oklahoma City was a shocking demonstration of domestic terror. Natural disasters have taken their toll as well… Tornadoes have leveled parts of Kansas, Missouri, Tennessee, and Maryland. Ohio residents were hit with debilitating February ice and snowstorms. A massive natural gas explosion in Toronto reduced a strip mall to a huge crater. Wildfires in California, Colorado and Arizona destroyed homes and businesses and threatened the tourism industries in those areas.

In this climate, any organization that runs events should be prepared for anything that could happen – to protect its exhibitors, speakers, attendees, employees, and, to the greatest degree possible, the continuity of its events. Inherent in this is the impact on the organization's reputation. It's entirely possible that one ruined or badly handled event might mean years of rebuilding reputation and attendance.

The likelihood is that the event planner or manager is the person most likely to have to deal with any disruption to an event. This paper is aimed at helping those individuals prepare themselves to deal with the threats and hazards that might befall a conference or exposition and to prevent or, at the very least, minimize the impact of a disaster.

Toward that end, this discussion will focus on planning for disruptions. The following principles of emergency management, including the activities each might generate, are provided to guide your planning:

- Preparedness - activities involved in building awareness and assessing the risk of potential disasters
- Mitigation - activities aimed at reducing vulnerability; activities performed in advance to reduce impact, potential loss or damage
- Response - activities occurring during or immediately following a disruptive event to minimize the immediate impact(s)
- Recovery - activities to minimize long-term impacts and return the situation/system to the "new" normal

If you talk to any true emergency management professional, what you'll hear is an echo of this: have a plan and keep these principles in mind as you plan.

**Determining Risk**

Before you begin any kind of planning or assessment, it is important to determine risk… to decide on what potential disruptions to concentrate what are usually limited resources. It's not possible to be prepared for every possible disruption; you have to concentrate on what is most likely to occur. This universally accepted risk management equation will help with this effort:

***Risk = Probability + Consequence***

Probability, quite logically, refers to the likelihood of something happening, while consequence refers to its impact. For example, the probability of a meteorite hitting your event facility is likely quite small, although the consequences from such an event would be huge. The risks on which you want to concentrate are those in which both the likelihood of occurrence and the potential consequences are in the medium to high range. Keep this in mind as you go through the emergency management process.

Most of all, keep things in perspective. Any consequence that involves potential critical injury or loss of life must take precedence over less critical outcomes. It's important, therefore, to prioritize the risks as well as identifying the ones to focus on.

**Preparedness**

*Identify the vulnerabilities.* While many threats are equally likely to impact organizations (hurricanes, floods, food poisoning), each organization usually has unique threat potential from groups that take issue with its practices, beliefs, etc. For that reason, it's important to assemble a group of key organization and event players who are aware of and can help identify issues or activities that make the group vulnerable to specific vulnerabilities. This is the stage during which potential threats are identified, their individual risk is assessed, and a comprehensive list of vulnerabilities for which to plan is developed.

If this seems like a daunting task, it also is extremely rewarding when your planning results in successful handling of disruptions. Another benefit of this step is that some vulnerabilities can be eliminated simply by knowing about them beforehand. For example, if your drayage company or "official airline" has a union contract scheduled for renegotiations during your event, you might want to change companies or line up backup in the event of a strike.

*Be aware.* You know your event will be held in City X or Country Z in eight months. Follow what is going on there locally - are there potential situations that could impact or interfere with your event? Will there be other events at your chosen facility while you're there that might result in demonstrations, bomb threats, etc., which could impact your event? If so, perhaps you need to line up a contingency location. You certainly will need to know about local resources. Communicate with the facility management to determine their awareness of vulnerabilities and plans for dealing with them. The situation in your destination city and facility also should be factored into your plan.

*Develop a plan for each scenario identified - and TEST IT.* The planning isn't as difficult as it sounds. You really need one basic plan that can be customized for each different threat/hazard, because a lot of the planning or information used in the planning will be the same no matter what the disruption. You can't possibly test these plans completely because you'd have to be at the facility to do so, but you can do simulated run-throughs that will help you determine if things can work. And, if your budget allows, it really wouldn't be a bad idea to make a trip out to your chosen facility and get their people to participate in the test phase. At the very least, share your plans with them and get their input as well.

How do you plan? Take the case of a bomb threat, for example. Although the majority of bomb threats are false (we are told), who can afford to ignore such a threat? Use a scenario in which you are told, at 1 pm on the opening day of the conference/expo that a bomb threat has been called in to the facility. What's your first question? (When is the bomb supposed to go off?) If the answer is in 20 minutes, that's Plan A; if it's three hours from now, that's Plan B. The most critical thing to consider is how to handle the situation with the least risk to life. So, if you have three hours and your research with the facility has indicated it will take 35 minutes to evacuate the building, there's the answer. If you have 20 minutes, now what do you do? This is the kind of thinking that you have to go through to survive the disruption and be able to carry on if possible.

**Mitigation**

This is the area of planning with the highest return potential, but one in which people seem to spend the least time and effort. What is mitigation, exactly? It's everything you do to prevent a disruption from occurring or to minimize its impact. It's keeping your virus protection updated, for example, to prevent data loss from a new virus. It's planning early and carefully for security at your event. It's having a backup plan in case your registration system goes down an hour before registration opens. It's having a complete list of contact phone numbers so you can reach anyone on the event staff or anyone else necessary at any time of the day or night if something comes up.

A lot of mitigation is accomplished through communication. If a situation in a given area is threatening to reduce event attendance (SARS in Toronto, for example, or terrorist activities in a foreign location), it's communicating to attendees that the area is safe and why - or that the event will be moved if things deteriorate to a specific state. If they know you have their health and safety in mind, they are more likely to attend. Communicating to convention center personnel and event staff is just as important.

One attendee at an IAEM event (a convention center person) talked about having a plan, but most people didn't know what the plan was and no one had practiced using it. This all came to a head when tornadoes blew through town and no one knew what to do. The good news is that no one was hurt and no damage resulted. Even better news: now they communicate the plan and have quarterly drills.

Another attendee used mitigation activities to contain a demonstration that could have disrupted a graduation ceremony. The group came looking for publicity for their cause and, because they had notified

the facility of their plans, management was able to set aside an area for them to protest and be seen by media but prevent total disruption of the graduation.

Mitigation activities can be identified by reviewing the list of vulnerabilities and/or the plans to determine what can be done NOW as opposed to waiting for a disruption. This kind of planning is one of the best ways to help ensure your "event continuity."

**Response**

When the firetruck comes, that's response. The response period is when the disrupting event happens, from the point of activity to about 72 hours later. You need to build response capability into your plans in order to minimize the immediate impact of any disruption. If the hotel your attendees are staying in burns down while they're at your keynote address, what are you going to do? (Yes, you will be the one they're looking to for guidance.) You can't tell them it's not your problem… you'd better be on the phone finding other accommodations and helping them figure out how to replace their personal belongings, how to file an insurance claim with the hotel, and how to replace their lost medications. If you find that the hotel has all this planned for, then your job will be to find out how to get your folks into the system.

You can best handle the response to any disruption if, in your planning, you created a crisis response team that you can call into play. Just as you can't possibly plan for every vulnerability, you can't possibly pre-determine responses when something like the hotel fire occurs. But you can translate other plans to help you deal with this, and you can hold drills to practice working under pressure and as a team. If someone doesn't react well, get them off the team; someone could die if an individual becomes a loose canon. What you need on this team are people who can keep their heads, who are resourceful, and who can move quickly. You also need a spokesperson - someone who will deal with the media (when necessary) and attendees confidently and forthrightly.

In one instance, a non-life threatening disruption happened when a show's registration system crashed just as the registration process was opening the evening before the show. Quick thinking on the part of the event staff (and a good budget) saved the day, when catering was contacted to bring out food and drink while the staff handled registration manually.

One thing to remember in the area of response to threats and hazards is that despite different causes, the general flow of activities is similar. There is an "all hazards approach" - try to save people, secure the situation, get everything under control.

**Recovery**

After any disruption, all we want is for things to "get back to normal." Be prepared, however, for the fact that this seldom if every happens. After any disruption, there is usually a "new" normal. Things have changed. A classic example of this is the impact of 9/11 on the businesses surrounding the World Trade Center. There were restaurants, dry cleaners, newsstands, and other shops that were able to

reopen, but without the several thousand customers who used to populate the World Trade Center. The ones that did reopen now have a “new” normal.

We want whatever we do in the recovery stage to enable us to minimize the long-term impact of the disruption on the event and the organization. In the case of our hotel fire, above, recovery might mean making sure that everyone who was affected has received all the help possible from the hotel and the event management to prevent them from swearing off your event forever. The fire wasn't your fault, but they will look to you to follow through on whatever action was initiated at the time.

**Summary**

Your job is an overwhelming one, when viewed from the perspective of planning to survive the threats and hazards that can impact events. Planning is the key to making it through. The risk assessment and emergency management processes are tools that you can use to identify and prepare for the myriad of disruptions you might face. In the next sections of this paper, we have provided (1) a list of potential threats and hazards to help you think about what to plan for and (2) some resources that will assist you in developing those plans and your responses to any situations that arise.

**Threats and Hazards: A Sampling**

Please note that this listing ("Avoiding Disaster" by John Laye, pp 30-32) is meant to help you generate your own lists of threats and hazards, for which you need to determine your risk and then develop your plan. It is not a comprehensive list, but one that we hope will provide a basis for discussion. We have broken this list into the following categories: (1) Natural disasters, (2) Accidental/Technological, and (3) Man-made/Human-caused.

1. Natural Disasters

- Hurricane / Typhoon
- Tropical Storm
- Earthquake
- Floods
- Tornado
- Winter storm
- Hailstorm
- Landslide
- Avalanche
- Wild land Fire
- Volcanic Eruption
- Solar Storm
- Drought
- Wind storm
- Tsunami
- Epidemic

2. Accidental/Technological

- Cyber outages
- IT System Crashes
- Supply Chain Failure
- Hazardous materials
  - Stationary source
  - Transportation
- Major Fire
- Building collapse
- Dam failure
- Infrastructure failures (communications, sewer, water, power)
- Transportation disruptions (air, highway, pipeline, rail, water)

3. Man-made or Human-caused

- Bomb incident
- Civil disorder
- Extortion
- Theft
- Arson
- Missing funds
- Kidnapping
- Protests
- Contamination (biological, chemical, radiological)
- Cyber attack
- Deliberate destruction to basic infrastructure
- Chemical, biological or radiological attack
- Epidemic
- Regulatory/Legislative (Homeland Security/Patriot Act, European Union)

## Resources

The following is a list of resources that we feel may be helpful to you in your planning.

American Red Cross - www.redcross.org

Department of Homeland Security - www.whitehouse.gov/homeland/

Federal Emergency Management Administration - www.fema.gov

National Terror Alert Resource Center - www.nationalterroralert.com

DRI International -- www.drii.org

The Weather Channel -- www.weather.com

Center for Disease Control -- www.cdc.gov/

The Hartford's "Weather-related and Natural Disasters" -
http://www.sb.thehartford.com/reduce_risk/loss_library/Weather_Related_Natural_Disasters/

Book: "Avoiding Disaster" by John Laye
http://www.amazon.com/exec/obidos/ASIN/0471229156/attainiumcorp-20

Attainium Corp - Business Continuity, Disaster Recovery & Emergency Preparedness
Resources -- www.attainium.net/resources
Weekly NewsBriefs -- www.attainium.net/newsbriefs

**Source:**
**Bob Mellinger**
**President**
**Attainium Corp**
**Phone: 571-215-5276**
**Fax: 703-991-8462**
**Email: bmellinger@attainium.net**
**Web: www.attainium.net**