Friday, March 22, 2013
Workshop Session 5
Time of Session: 1:30-3:00 PM
Session Title: The Decision-Making Process (Interactive Session)
A. Crisis Gaming as an Element of Risk Mitigation and Organizational Resilience: A Case Study of The University of California, San Diego

Speaker: Phillip Van Saun, University of California, San Diego
Room: 257
Head Count: 7
Note Taker: Mariana E. Marmol

The author talked about gap analysis strategies to educate all those that live and work in the academic setting (i.e. faculty, staff, administrators, and students) understand crisis management by engaging faculty and students through a series of gaming scenarios. Students are engaging in these practices at the University of California, San Diego; therefore, Van Saun is hopeful that in 20 years they will be teaching crisis management strategies in the University Setting.

Author emphasized the reasons for and the "how tos" for Crisis Management. Organizations that already have a response plan were reminded about the importance of understanding why a framework, forms, and practice are not just nice to have, but they are must haves. Van Saun also provided sound advice on building both crisis management teams and 'all-hazards' based plans and gives strategic crisis communications guidance including sample talking points. He explained the steps to conduct crisis gaming and how to conduct a needs assessment to ensure that an organization has carefully mitigated all identified risks.

Techniques are taught through experiment-discussion based, case studies. Demonstrating the process of gaming starts with questions not set scenarios.

- Understand how to make decisions when a crisis strikes, in other words, when information and resources are limited.

- Encourage risk sensing
  - Educate faculty, students, and staff how to sense risk! Currently, the college population is not actively searching for risk, so that any crisis would take them by surprise.

- Take a step

- Mitigation

- Walk through process → learn by doing

The process begins by collecting intelligence. Though good and necessary, raising awareness is not enough. This is where gaming scenarios come in. The Military is always gaming scenarios.

Some say that Universities are similar to cities, managed by a government. However, universities have an entirely different dynamic so that a chancellor/president is not at all like a mayor. Therefore gaming scenarios that are more realistic to the University setting require that we consider the following:

1. What keeps you up at night?
2. Present possible solutions
3. Discuss challenges
4. Think about realities and determine possible moves taking into account your culture
5. Select some moves given realities
6. Implement steps to mitigate risks

The Physical environment
Do not assume rational (linear) action. Walk through the process, which might be convoluted. Checklist processes are not enough. Identify gap between understanding and application. Crisis management is not being taught. Teach difference between intelligence and information.

Message mapping: taking academic learning and applying it. i.e. ICS

Synthetic organizations are good Samaritans and do good things when bad things happen. Train people the crisis-decision process to be able to do good things when bad things happen.

Sometimes information we have is fragmented and you have to react counteractively.
   - Learning to trust your gut
   - Traditional excercises are sometimes too structured
   - Useful tool
   - Convoluted process could get out of hand

Micro-Game (Interactive)
   - Focus on strategy: Do not think tactics; people will defer to tactics because it is comfortable. Don’t worry about EOC.
   - Brainstorm
   - Open discussion: no one has all the answers
   - Set / identify the goal(s)
   - Suspend disbelief
   - The scenario is plausible
   - Events do not occur in real time

The Basic Game Flow starts by defining or determining when we have reached a crisis, or when a situation has reached harmful potential.

Indications and Warnings of a Crisis:

   - What management system will you use to respond to this scenario?
   - Who is in charge?
   - What is the message?
   - What are the short-term recovery issues? Long-term?
      ○ Reputational risk