

## When Crisis Strikes: 10 Steps for CEOs

Posted by: Hugh Hewitt at 7:49 PM  
Sunday, November 30, 2008

My friend Frank Dowse is the head of [Agemus Group](#), a security-consulting firm. Frank's been in the business since his retirement as a Lt. Col from the Marine Corps a few years back.

Frank was my guest on Wednesday's show as the terror attacks in Mumbai were unfolding. I asked Frank what a CEO should do when he discovers he has employees in an area where a crisis develops. Frank sent along this follow-up:

I would like to provide for you and your audience a more direct answer to the question...which was (paraphrasing) ***"If one is a CEO/COO tonight with people in Mumbai, what can they do?"*** I'll preface this with the situation that the attacks are already underway, and that the CEO is reacting, vice mitigating or preventing, security and crisis challenges in the future. A planning assumption is that there is communication with one's employees, or at least we know what hotel they are staying, and their basic schedule of events.

***"I felt totally helpless... What was needed was a Crisis Management Group in addition to the National Authorities to deal with this crisis"***

**Ratan Tata, CEO of the TATA Group, owner of the Taj Hotel, Mumbai, India**

1. **Initiate/Designate a Crisis Response Team:** If this is not an inherent function or area of responsibility within your organization, then assign a Point Man (COO/Vice President Level, with PR reps to assist) who can lead, authorize, and decide on behalf of the management, in order to best affect plans and responses as events unfold, and information is gathered. This needs to be a 24 hour operation, and should be given top priority for resources, and manpower.
2. **Start a Log,** capturing time lines, significant events, persons, and exterior contacts and players.
3. **Accountability:** Find out where your people are, and their condition, and ability to rendezvous with representatives of the company, or a trusted agent/or Embassy personnel. If determined they are not mobile, then advise them to "stay put" and minimize all contact with strangers, non official security personal. **Advise them to silence their cell phones.** Provide updated, vital information only as it pertains to them specifically. Have your staff establish contact with the US Embassy (or respective embassy) and pass info on who has been accounted for, and who is still missing. Inquire with both local and National authorities as to how businesses, and you specifically, can assist in the recovery and accountability of your people. If it was not emphasized already, the employee should be instructed to make periodic "on deck" calls after transiting, or executing a scheduled event. If there has not been a "check in" call, then it is encouraged for the staff to "text" if possible, and inquire as to the status, whereabouts, and wellbeing of their employee.

4. **Establish Contact with Families/Significant others:** If information is forthcoming (from the Embassy, federal authorities), tell what you know, and ensure it is not premature, rumor, or simply press reports. Ensure the Crisis Response team is the “releasing” authority for all info coming from the team. Keeping the families in the proverbial “loop” is one of the most important and valuable things an employer can do in a situation like this. This is best accomplished if a “pre-trip” brief has been conducted, in which emergency info and contacts are acknowledged, and the (now) victims have agreed and know that the people who have the need to know their status will, in fact, be contacted.
5. **Draft and release a company wide alert** as to the situation unfolding, and ensure all “deployed” employees, and those living and working overseas have reviewed and initiated preliminary anti terror, employee protection measures and procedures. If there is credible information that this could become more wide spread, or inter-regional, recall your people to a safe location, and ensure they are accountable as well. Personnel should be made aware that this is a serious warning, and it needs to be adhered to.
6. **At a minimum, the company should review all extended travel arrangements** for its personnel abroad, and conduct a risk analysis/cost benefit assessment as to the necessity and gain from any extended travel.
7. If persons are to travel, they **should have a means to contact their respective chiefs and offices and their contact information for their chiefs**, numbers to the US Embassy, providing detailed departure and arrival schedules for their Chiefs, and have a plan for alternate routes and times for their routine travel plans.
8. Have the Crisis Response team **begin developing procedures (action plans)** that can be implemented (color coded, numbering system, “Severe, Critical, Heightened...etc.) that already embody and explain the levels of internal travel restrictions in a concise, clear, and direct manner, so there is no confusion as to the expectations of management on employees.
9. If persons must travel, **assess the security environment** for the area to be traveled, and **review Personal Protective Measures and Levels** (escorts, Secure Transportation, Hardened Vehicles).
10. As the crisis subsides, **appoint a senior member of the company to evaluate and recommend retaining an experienced Crisis Mitigation Firm with international experience.** (A little self serving, but honest) They need to be experienced enough to deal with, or refer as necessary to the qualified and trusted networks, international crisis and security challenges. **Come to grips that the global business environment as it was known, is forever changed,** and CEO/Senior managers can no longer afford to “hope” something will not happen. Also, review and analyze impact of the **landmark legal case of Timberwalk v. Cain**, which highlights that an environment prone to terrorism may be determined by either of two types of legal notice: Actual, by real events on property or territory; or constructive, where factors such as proximity of events and general deterioration of environment are reviewed. The availability of notice creates possible legal exposure for companies that have not properly assessed and mitigated their terrorism risk using readily available analysis tools or programs.