

February 3, 2009

Opinion – Security

Corporate Insight

## Time to act, not just react

*Debashish Sengupta*

If the global financial crisis and the Mumbai carnage were not bad enough, the new year saw the 'lid' being blown off the big 'Satyam scandal'. Corporate coffers have, no doubt, borne the brunt of these unwelcome developments but those affected the most by these upheavals are the employees. They not only have to combat the fresh set of changes and challenges, but also have to confront heightened risk of job loss, and financial and physical insecurities.

Smart planning can, to some extent, offset the impact of job and financial insecurity. What is more difficult to deal with is the physical insecurity that an employee faces, especially in the light of the 26/11 Mumbai attacks.

The very fact that workplaces in India face such a high degree of vulnerability has sent shock waves among the general public. Though some organisations have woken up to this issue and put better safety systems in place, there are still certain worrying gaps. Some of the gaps identified in employee security practices are:

**Use of primitive security systems:** Most companies use primitive security systems. They do not have access to state-of-the-art security gadgets, partly because of ignorance and partly due to cost-concerns.

**Lack of properly trained security personnel:** Most security personnel are poorly trained and not exposed to the exponentially enhanced threats of global terror. Many companies outsource establishment and employee security to private security agencies but fail to monitor the quality or skill-level of the personnel.

**Lack of motivation among security personnel:** Most times, the security personnel are not adequately compensated and have long, stressful hours of work. At times, the facilities given to them are inadequate; security personnel in some firms do not even have access to restrooms.

**Complacency:** The heightened security checks and alerts that one witnesses in the light of any terror attack often fade with time. Such complacency is contagious and criminal.

**Infrastructure issues:** Many offices do not meet the stipulated infrastructure norms to ensure occupant security. Offices with single entry and exit points are nothing short of concrete traps in the event of a crisis. Fire-fighting systems are created most of the time to meet official norms, rather than ensuring real effectiveness.

**Lack of employee concern and co-operation:** The final straw comes in the form of the employees themselves showing a lack of concern and cooperation, at times towards the security initiatives taken by their companies.

'Piggy-backing' is another growing problem, where an employee uses his own access card/rights and another enters without using his own access permissions. This poses problems in security monitoring.

Employee security is a responsibility and challenge that companies can no longer turn a blind eye to. This issue requires proactiveness, seriousness and preparedness. It is time we 'act' and not just 'react'.

(The author is Chairperson, Human Resources Area, Alliance Business School, Bangalore.)