



PRESS RELEASE

Stringent 'threat analysis' and multi layered security approach required for Indian companies: KPMG survey report 2009

No 'vulnerability analysis' in place by large number of respondents, only 33% of those under the survey conducted such an analysis

Only 24% of the respondents have comprehensive response plan for a possible security incidence

Over 85% of respondents believe corporations need to give cognizance to terrorism in building their security plans

Only 39% of the respondents have insurance cover for terrorism related incidents

Anti money laundering (AML) efforts critical to curb terrorist financing

New Delhi, January 16, 2008: Corporate India is not prepared to cope with a security incidence in case they are caught in a terrorist attacks or are faced with an unconventional threat, reveals the latest KPMG survey conducted by the Forensic services practice. The survey results draw attention to the fact that gaps exists in the current security measures of most companies indicating a need to improve the current security framework.

Although the fight against terrorism might be seen primarily as the role of the government; with corporate assets and executives becoming vulnerable, organizations can no longer treat organizational security as a mere administrative issue. Corporates should assume a more proactive role in ensuring that at organizational level they are accountable for the security of their premises and personnel and do not become victim of such attacks on account of negligence.

The survey conducted by KPMG with select companies in India from various sectors , majority of them with an annual turnover of over USD 150 million, assesses the level of preparedness of these companies in the wake of emerging threat of terrorism. The survey reveals that more than half of the respondents (53%) did not conduct such threat analysis. Only 1/5th of the respondents had conducted such a threat analysis. The preparedness to threats was also found to be

drastically low with, only about a quarter (24%) of the respondents had a comprehensive response plan and rest of the respondents either had no or very generic security response plan for their organization. A vast majority of the respondents said that these plans are just documented and neither employee's are aware about it nor do they conduct regular trainings.

Speaking on the release of the report Mr. Deepanker Sanwalka, Head – Forensic Services, KPMG India said “Organizations across the globe are obliged to provide for a safe working place, therefore, it is imperative that corporates draw effective emergency plans to ensure proper safeguards for their employees, assets and business.”

The survey reports bring to light the non consideration given to terrorist attacks even in the Business Continuity Management (BCM) plans of over 58% of the respondents. BCM is a critical process for organizations since it helps them recover expeditiously post an occurrence of a disaster or an extended business interruption. Almost 60% of the organizations think that they can reduce the risk of such threats by taking appropriate measures. Another 34% were of the opinion that measures would have limited impact, while a meager 7% of the respondents said nothing could be done at the organizational level to avoid such risks. When asked to rate security related aspects – background verification of employees was deemed the most important aspect followed by IT and perimeter security. Due diligence of vendors/ service providers followed by training and perimeter security were identified as the weakest area within the organizational security. Only 14% of those surveyed said that they did not conduct background verification on their employees while 35% said that no background checks for vendors are undertaken.

According to the respondents travel (airlines/airports), hospitality and retail are more prone to terror attacks as compared to others. These the respondents believed were soft targets due to sheer volume of people visiting such places and easy access.

The KPMG report also delves into Anti Money Laundering and the allied issue of terrorist financing. One of the important features of terrorist financing is concealing the source and usage of funds. The KPMG report suggests that in order to successfully tackle money laundering, it is critical that there exists a joint approach between the private and public sector. What is needed within the banks is clear understanding of the typologies used by money launderers, the risk factors they should consider while identifying these, as well as intelligence in relation to individuals and entities.

Some recommendations from KPMG to mitigate risks (please refer to the report for the complete list)

- Conduct a threat perception analysis for all locations in order to assess the exposure to the risk
- Consider terrorism as a major risk when designing disaster management and BCM processes
- Thorough background checks of all employees
- Training people for emergency response when a disaster strikes
- Continuous engagement with Intelligence agencies to understand the alerts and react appropriately
- Educating IT users with risk management principals and countermeasures in case of a disaster or a terrorist attack

For further information contact:

<p>Subir Moitra Senior Manager–Marketing & Communications KPMG – Delhi Mobile : +91 98111 99613 e-Mail : smoitra@kpmg.com</p>	<p>Archana Dabral Senior Manager- Marketing & Communications KPMG - Mumbai Mobile : +91 98200 04441 e-Mail :archanadabral@kpmg.com</p>
---	--
