



Ensuring Business As Usual in the Face of Terror

Understanding & Adapting to a Changing Security Environment in India

THE MACRO PERSPECTIVE – DOES TERROR IMPACT COMMERCE?

Since the tragic events of 26 November 2008, there has been much said about how there is a clear linkage between terror activity and economic performance of a nation. Indeed, the choice of the terrorists' targets – in terms of Mumbai and the specific locations within Mumbai – seem very heavily influenced by the desire to create an impact on the Indian economy; and try to shake the confidence of Foreign Institutional Investors (FIIs) in the strong Indian growth story.

Hit with its most prominent terror strike ever in the midst of one of the largest global economic downturns seems to have been, at the surface, a “double whammy” to the promise that India holds as one of the world's leading emerging economies.

In our opinion, nothing can be further from the truth. India has had a long history of fighting terror; and her rapid economic growth since the early 1990s has taken place despite the continuing prevalence of terror. Many significant terror events – such as the Mumbai blasts of 1993, the New Delhi blasts of 2006 & 2008 and the Bengaluru blasts of 2008 – aimed at creating a dent in the Indian growth story have failed to arrest India's strong economic growth.

INDIA'S PATH TO GROWTH AS AN ECONOMIC SUPERPOWER

India embarked on the era of economic liberalization and, consequently, rapid growth in 1991, when India's then-Prime Minister, P.V. Narasimha Rao, chose (current Indian Prime Minister) Manmohan Singh to be the Finance Minister of India. At the time, India was facing an economic crisis; and Rao and Singh decided to open-up the Indian economy and change the socialist economic system to a capitalist economy. The economic reform package included implementation of policies for private businesses to exist and prosper, promoting Foreign Direct Investment (FDI) and initiating the process of the privatization of public sector companies. These economic reforms are credited with bringing high levels of economic growth in India, and changing the annual 3% to an average of 8%-9% growth in the coming years.

Leading policy makers and analysts are confident that despite the global economic meltdown, India will continue to grow at over 6%.

GROWING DESPITE TERROR

This growth is despite the multiple challenges faced by India as a result of terror strikes and ongoing “organized” acts of violence allegedly by foreign and indigenous groups. Just in 2008, five prominent terror attacks have taken place viz.

- May 13 blasts at Jaipur with 51 victims
- July 25 at Bengaluru with 9 serial blasts
- July 26 at Ahmedabad with 16 serial blasts and 29 victims
- Sept 13 blasts at Delhi with 21 victims
- Nov 26-27 attacks at Mumbai with 199 victims

In addition, India has witnessed ongoing strife in various localities; such as the “Naxalite” movement in the eastern states of Bihar, Orissa and Andhra Pradesh; and separatist movements in the north-eastern states of Nagaland and Assam.

Increasingly, the terror activities, which are escalating but sporadic pan-India activities, seem to be aimed at creating civil unrest and secular division; and at identifying high-profile, often western-oriented areas to target.

ZERO IMPACT?

While the Indian economy in general, although not insulated from global economic downturn, is likely to continue to grow despite terror attacks, the focus on security is very high. India is, at the highest policy making levels, implementing several initiatives to enhance its protection against terror attacks. A landmark bill, outlining several tough counter-terrorism measures, was passed by the Lok Sabha (House of Commons) of the Indian Parliament on December 17, 2008.

Therefore, while having a low impact on current market sentiment, the terror attacks have brought into focus the need to have a proactive and strong mechanism to enhance safety and security.

This need is accentuated by perceived flaws in the Indian Federal security apparatus. The Central Government is responsible for external security

through arms such as the armed forces, Border Security Force, Coast Guard, Central Reserve Police Force and other military and para-military units whilst State Governments are responsible for internal security (except for borders and international waters) through local police and other allied units. Intelligence, a key aspect of security operations, comprises both central and state level bodies. Doubts have been raised about the level and efficacy of coordination and communication between these agencies. In general, the following are perceived as the general challenges with respect to the security apparatus in the country:

- Lack of coordination
- Inadequate flow of information
- Multiple agencies for coastal defence e.g. coastguard/Navy/State Police
- Serious response to external advisory both at Centre and State level
- Inadequacy of State agencies to handle high-level terrorist threats
- Multiple ingress points/ 2,000+km coastline/porous borders & open borders
- Post partition and religious/ethnic divide

Considering all of the above, the commercial sector in India is now re-energized to boost security which is sometimes viewed as a wasteful expenditure with low contribution to the bottom-line.

The commercial sector realizes the essentiality of strong security solutions to protect against now real threats such as:

- Bombing
- Postal (Anthrax, Letter-bombs)
- Food Poisoning
- Sabotage
- Armed Attacks
- Kidnapping and hostage situations
- Car Bombs (ramming)

ADDRESSING THE ISSUE

The age-old cliché “prevention is better than cure” appropriately sums up the ideal method to respond to the threats posed by terrorism. Prevention in this instance covers:

- Prudent **risk management** methodologies – proactively identifying risks and mitigation methods
- Applying **security considerations** in everyday operations and ingraining them in the cultural fabric of the organization
- Putting in place **preparatory measures** to ensure prevention of terror attacks

RISK MANAGEMENT

The primary endeavor in risk management is reviewing property and associated security measures. A detailed security audit of facilities and estates with a renewed focus on identifying potential terror-related threat points is key to the development and execution of appropriate risk management practices. Typically, this audit should include the following:

- Reviewing existing locations and relocating from high risk / low security sites
- Considering new business locations at major parks / estates with central security and access control; finalizing locations after inputs from security consultants
- Identifying proximity of adjacent buildings (and ensuring your neighbours plans are complementary with your own)
- Accessibility for air evacuation and transport for military response
- Encouraging the spread of senior management around the building
- Appropriate access control practices
- Protection to be provided to security posts
- Regular reviews & audits with enhanced periodicity and physical checking
- Training of facilities personnel on what to look for in building inspections from a security threat perspective
- Mailroom scanners and training to mailroom operatives on mail handling
- Screening “cook chill” hot locks and incoming food supplies
- Testing and keeping food supplies for 24 hours for traceability purposes
- Locating meeting rooms / visitor interaction areas away from work areas
- Creating adequate means to restrict access / movement between building zones

- Regularly test emergency response preparedness and establishing links with emergency services

It is also critical to ensure that the right partner be chosen for facilities services and other related services which involve a high degree of vendor staff presence. The impact of employing a contractor or even a reputed service provider who sub-contracts to vendors with inadequate controls on employee integrity and background creates a significant exposure for the overall security level at the facilities. For instance, with the risks surrounding catering, it is critical to have a service partner who is able to ensure that no risk of poisoning emerges right from the sub-contractor level.

Each element of the facilities audit requires a high level of detail, unique to each corporation and each facility; however, it is sound practice to have standard mitigation strategies which once translated into policy, are then customized for each individual facility as required. For instance, on access control, the practice could include the following:

- Gates and traffic controls to be located on main roads
- Vehicles to be stopped at a distance
- Quarantine areas to be created for essential vehicles
- Embedded gate barriers to be built for vehicles which ram main gates
- Boundary wall heights to be increased and landscaping / shrubbery around the perimeters adequate maintained to ensure clear lines of sight
- Alarm and SOS buttons to be installed at gates, reception areas and other potential areas of unauthorized / forced ingress
- Security equipment present at site to include scanners, vapour detectors, vehicle scanners, bag scanners and electromagnetic emission detectors amongst others
- Appropriate training to be provided on use of security equipment (eg. on vehicle scanners – vehicle underbelly profiles, wires, new shiny devices)

APPLYING SECURITY CONSIDERATIONS

Taking clear steps towards ensuring that security concerns are taken into account by every corporate department in each aspect of their functioning requires discipline and continuous reinforcement but will significantly enhance the security of the environment. Illustrations of such considerations include:

- Bifurcating internal and external security teams as each require different skill-sets; and ensuring that adequate specialist training is provided on tenets of internal / external security practices in addition to basic training courses
- Improving communications and establishing protocols to ensure that the chances of information leakage – a key contributor to terror attack planning – is prevented
- Provisioning for additional security manpower at the time of shift changes and other events to ensure that all posts are adequately manned and enhanced vigilance is achieved
- Establishing a mechanism to ensure the swift sharing of information relating to possible threats between corporations, security agencies and district administration
- Involving Human Resource departments as a key ally in the security process

The last point on the above list is especially relevant since the recruitment and related background check formalities in any corporation usually rest with the HR group. HR can play a key role in creating a secure environment through the following:

- Cutting down, preferably eliminating, “walk-in” interview sessions
- Ensuring comprehensive employee screening which goes beyond just police checks by employing a reputable agency for physical check of antecedents and background, visiting villages, checking for pro-terror sentiments / leanings in family and checking to 3rd cousin level where possible
- High emphasis on checking antecedents of vendor staff and creating other mechanisms for contractor control
- Looking for susceptibility and strong leanings and beliefs amongst staff members on an annual basis
- Looking for tell-tale signs (such as personal lifestyle not being commensurate with available means of income) – again on an annual basis

PREPARATORY MEASURES

Being prepared can ensure that many potential sources of terror strike are nipped in the bud. Some of the most effective preparatory measures that a corporation can employ include:

- Key corporate staff dealing with contingencies to be specially trained by central/ state agencies
- Educating staff on basics of survival techniques
- Emergency Response planning and training; training tailored to facility; sensitive to environment with physical and verbal communications
- Emergency ration and survival kits for protracted stay.
- Easily available ambulance and trained nursing assistant
- Stock of field dressings (just first aid boxes are insufficient) on site and in transport
- Well-trained Floor Marshals who are thoroughly drilled on SOPs and are senior enough to be listened to
- Mock drills ensuring regular practice with variable exit patterns; segmented evacuation for possible scenarios – partial, phased and directed, set up safe rooms
- Establishing different evacuation points for fire, terrorist and force majeure events
- Creating a protocol and back-up equipment for effective communications during evacuation
- Personal protection/Exit Plans

IF IT HAPPENS...

Despite best precautionary measures, should a corporation be the target of a terror strike, a structured approach can help corporations respond in a manner that minimizes impact on life, business continuity and brand image.

Issuing a response procedure to all employees with the following practical tips forms the primary action item on response to terror strikes:

If out of terrorist line of sight:

- Turning off lights – the basic step which helps occupants of a building gain advantage in terms of moving around undetected and ensuring that they aren't visible to a gunman or external sniper. Internal area security teams can be trained in this critical first step

- Barricading entrances – using furniture, especially heavy furniture, to block doors to the office area where the employees are hiding and latching all windows shut
- Ensuring that phones are in “silent” mode and using phones only for emergency calls to ensure that battery life is not wasted
- Lying down / taking cover – this is especially useful when hiding behind heavy furniture as bullets from many modern personal weapons are not designed to penetrate thick wood at close range
- Marshals trained to identify safe points and move people not in line of fire to the safe points. Safe points to be stocked with adequate supply of first aid and other medical supplies

On encountering a terrorist:

- Find nearest cover (ideally heavy furniture, landscape elements such as rocks, stone frontage, etc.). Do not try to outrun the terrorist
- If injured, pretend to be dead
- Offer resistance if attacked; common practices include charging the terrorist in a group if possible; or throwing objects at the terrorist to distract and / or injure

It has also been witnessed that, on occasion, terrorists target post attack congregations – such as hospitals or vantage points where people are gathered. In this context, another prudent measure is issuing advice to employees that, if not in the facility, or after escape from the facility, it is ideal to stay away from congregations.

In recent events, it has also been noticed that counter-terrorism security forces have faced challenges in two key areas:

- Identifying the number of hostages / occupants of the buildings
- Getting precise information of the building’s layout including external & internal ingress and egress points

In this regard, two other key initiatives include:

- Nominating a contact person (potentially from the security / facilities team) as the point of coordination. This person should maintain a list of employees at the facility updated as often as possible with attendance records. Any employee who leaves the facility should be instructed to call this single point of coordination to report safe exit from the facility
- Maintaining detailed maps of each facility offsite in such a manner that they can be rushed to the facility under siege and help security forces draw up action plans

IN CONCLUSION

Living with terrorism is a reality in India today as in most other parts of the World. Developed and emerging economies such as India will continue to be targets for terrorists who would like to use the attention as a means of propaganda and destabilization of regimes and economies.

Staying prepared is the best way to resist the terrorist threat and is a true reflection of the “the more you sweat in peace, the less you bleed in war” approach. Often, it is the inadequate/improper application of those basic security principles which every corporation should employ which enables such incidents to occur.

The India story remains strong. With enhanced security awareness and investment in security infrastructure and the preparation and protection of people and property, we can protect our economy, our business, our National and corporate brands and our lives.



Peregrine's Knowledge Initiative

*With over 13 years in the industry and a team of experienced, expert security professionals, Peregrine Guarding has a wealth of information, insights and analysis on security related responses to changing market, economic and social conditions. Just amongst our senior management team of 14, many of them from accomplished backgrounds in the armed forces, have over 300 man-years of security experience. We offer this expertise to the industry in general through **SecurCounsel**, our knowledge initiative and platform for ideas and thoughts on contemporary issues. The authors of this article are drawn from Peregrine's senior management team. Feedback may please be sent to corporate@peregrineguarding.com*

CORPORATE ADDRESS:

Peregrine Guarding Pvt. Ltd., Plot No. 13, Sector 18, Electronic City, Gurgaon 122 015

T: +91 124 401 9770 www.peregrineguarding.com

2008 © Peregrine Guarding. All Rights Reserved.

This case study is for informational purposes only. Peregrine makes no warranties, express or implied, in this summary.
Document Code: T/WP/A001/0908



PEREGRINE
a tenon company