

## Security Beyond the Protection of People and Assets - Taking a Holistic View

Security is a fundamental need, shared by people and organisations who wish to operate in an undisturbed and orderly environment. Managing security in large corporations, however, has become ever more demanding. Today's challenge extends beyond the protection of people and assets, requiring the management of multiple sources of risk and understanding the implications of one's own actions.

As companies expand internationally they become exposed to different societies with different values and different governmental and legal systems. How a company responds locally to new challenges in unfamiliar contexts is important, because it can have both local and international impacts. In an era of growing media scrutiny, and an increasingly connected global media, the actions of a local contracted security company can affect a company at its corporate headquarters. For example, an over-reaction by a security guard to provocation by environmental/anti-capitalist demonstrators could prompt allegations of human rights abuse, with resultant legal and reputational damage for the visiting organisation.

Over and above the laws of any given country, much of the relevant regulation around security provision is still voluntary. However, despite its voluntary status, contravening, for example, the Voluntary Principles on Security and Human Rights<sup>1</sup> or the OECD guidelines<sup>2</sup> will negatively impact the reputation of any leading firm. Furthermore, many of the component elements of these are being incorporated into formal legislation: organisations had better assure their compliance now, or be exposed in the future.

To take a more holistic view of security management, an organisation must understand the risks to 'visitors' of the country/community, and equally, the risks to the host communities. Security should be considered from three angles: the community, government policy/practices, and the protection of people and assets.

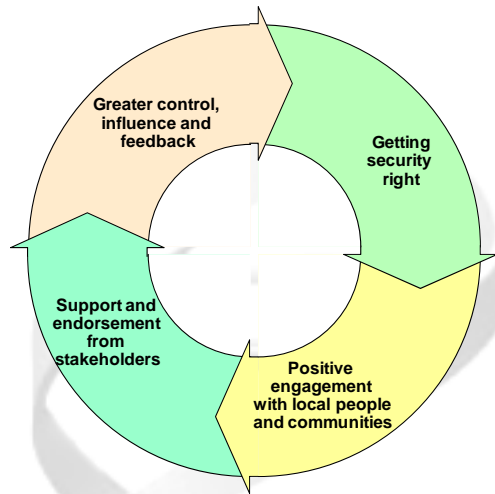
Many corporate security and human rights issues arise because companies fail to consider the potential impact of the business and their activities on people and communities. A Company must take proactive steps firstly to conduct an in-depth assessment taking into account their spheres of influence and control, and then plan their activities and stakeholder engagement to mitigate these risks as far as possible. Without effective stakeholder engagement it is not possible to truly understand community and government views or policies on security. Wide consultation ensures security is addressed in an appropriate manner. Communication is vital and should be carefully planned and managed to deal with cultural, legal and political sensitivities. If security is handled effectively, and stakeholder engagement is consultative and continuous, a positive security culture is created, creating a virtuous circle (illustrated in figure 1 below)

---

<sup>1</sup> <http://www.voluntaryprinciples.org/principles/index.php>

<sup>2</sup> [http://www.oecd.org/department/0,3355,en\\_2649\\_34889\\_1\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/department/0,3355,en_2649_34889_1_1_1_1_1,00.html)

Figure 1: A virtuous circle - Creating the right security culture



The integration of Security and Human Rights policies into an organisation's way of conducting business is often a major challenge. Leadership must send out the right messages and lead by example, training is necessary to build awareness and ensure consistency, and a clear understanding of the risks and impacts of a situation is required to build the capability to respond effectively to security matters, therefore building trust within local communities and governments. This, combined with carefully selected performance metrics that encourage the right behaviours, enables security issues to be managed effectively.

Evaluation and reporting on security performance will become increasingly prevalent. Organisations should keep up-to-date with published security and human rights best practice and develop their performance metrics accordingly. These metrics combined with a 'healthy' security culture should jointly serve to influence behaviours of people on-the-ground.

The diagram below illustrates a cycle of recommended activity:

Figure 2: Cycle of recommended activity - Creating the right security culture



The process involves establishing what needs to be understood, the cause of current or potential problems and the actions required to mitigate the causes. Performance should be continually measured and corrective measures put in place. A quick general analysis based on the above model is illustrated below:

Figure 3: A quick analysis - Creating the right security culture

<p><b>What do we need to understand?</b></p> <ul style="list-style-type: none"> <li>• Local attitudes to central government, police and the military</li> <li>• Local politics</li> <li>• Culture, language and religion</li> <li>• Society</li> <li>• Impact of operations and international perceptions</li> </ul>	<p><b>What can cause problems?</b></p> <ul style="list-style-type: none"> <li>• Failure to bring the community along</li> <li>• Loss of jobs and redundancies for local people</li> <li>• Company's lack of cultural awareness</li> <li>• Low environmental and safety standards</li> <li>• Community dependence on company</li> <li>• Ignorance</li> </ul>
<p><b>Possible impact/actions by community</b></p> <ul style="list-style-type: none"> <li>• Hostility - demonstrations, road blocks, etc.</li> <li>• Crime</li> <li>• Anti-company propaganda</li> <li>• Sabotage</li> <li>• Negative media coverage</li> </ul>	<p><b>Mitigating actions</b></p> <ul style="list-style-type: none"> <li>• Patience</li> <li>• Proactive engagement</li> <li>• Listen and understand</li> <li>• Only promise what can be delivered</li> <li>• Honesty and openness</li> <li>• Community partnering</li> <li>• Hiring of local people</li> <li>• Always remember you are the guests</li> </ul>

The holistic identification, prioritisation and management of security risk is key. To do this effectively requires an experienced team with a breadth and depth of security and relevant industry experience. The assessment is further strengthened by having a robust process, independent facilitation and practitioners that are familiar with the comprehensive risk assessment.

In conclusion, taking responsibility for managing security effectively lies with every individual and every business; it is the right thing to do. Organisations have a responsibility for their community footprint as an employer, investor or provider. Businesses should develop processes and practices to ensure they:

- Understand the totality of their risks at all times
- Never cause harm intentionally, or partake in any such activity
- Are aware of their sphere of control and sphere of influence and who is in it
- Maintain open, honest and consistent dialogue with stakeholders

In an environment where regulation may quickly replace good practice and guidelines, organisations must be prepared to respond appropriately, based on an understanding of the broad implications of their actions. They must ensure people and assets are secure, but think beyond this to be truly effective.

## *About i2a Consulting*

*i2a consulting helps clients improve performance through good business. Good business means meeting regulatory requirements and making responsible choices. Good business is about developing the right leadership and culture; using processes, metrics and systems to influence how people behave; and being operationally effective in getting the right things done.*

*i2a brings provides the right combination of expertise and process to help clients create effective security solutions. Our approach creates the virtuous security circle and the right security culture. We bring people together enabling knowledge, skills and experience to be used effectively to achieve positive results.*

*We approach security from a background of business consulting and improving performance. We combine deep expertise in critical areas with a proven ability to deliver behavioural change. Our clients get the right solutions working in the right ways.*

*i2a Consulting LLP, 22a Leathermarket Street, London, SE1 3HP.  
T: 020 7260 2930 E: [info@i2a.co.uk](mailto:info@i2a.co.uk)*

*© i2a Consulting*



***Good Business***