The Foreign Policy Centre

The Foreign Policy Centre is an independent think tank launched by Prime Minister Tony Blair (Patron) and former Foreign Secretary Robin Cook (President) to examine the impact of globalisation on foreign and domestic policy. The Centre has developed a distinctive research agenda that explores the strategic solutions needed to tackle issues which cut across borders – focusing on the legitimacy as well as the effectiveness of policy.

The Foreign Policy Centre has produced a range of **publications** by key thinkers on subjects relating to the role of non-state actors in policymaking, the future of Europe, international security and identity. These include: *The Post-Modern State and the World Order* by Robert Cooper, *Network Europ*e and *Public Diplomacy* by Mark Leonard, *NGOs Rights and Responsibilities* by Michael Edwards, *After Multiculturalism* by Yasmin Alibhai-Brown, *Trading Identities* by Wally Olins and *Third Generation Corporate Citizenship* by Simon Zadek.

The Centre runs a rich and varied **events programme** at The Mezzanine in Elizabeth House – a forum where representatives from NGOs, think tanks, companies and government can interact with speakers who include prime ministers, Nobel Prize laureates, global corporate leaders, activists, media executives and cultural entrepreneurs from around the world.

The Centre's magazine, **Global Thinking**, is a regular outlet for new thinking on foreign policy issues. Features include profiles, exclusive interviews with decision makers, and opinion pieces by the Centre's permanent staff and associated authors.

The Centre runs a unique **internship programme** – the UK's only route for new graduates into the foreign policy arena.

For more information on these activities please visit **www.fpc.org.uk**

About the author

Rachel Briggs runs the Risk and Security Research Programme at The Foreign Policy Centre. Her work focuses on how the changing security environment impacts on personal and corporate safety and risk. Her report, *The Kidnapping Business* puts forward a practical policy agenda for all the major groups affected – the Foreign Office, business and NGOs. The report received considerable attention among these policy groups. As a result of the report, the Foreign Office has changed the way it organises its travel advice for those visiting hot-spot countries, and the report is used as a training tool for NGOs exposed to the risk. *Travel Advice* discusses in wider terms the content of Foreign Office travel advice and the extent of personal responsibility, the report argues that if the Foreign Office is to continue with its current responsibilities to Britons overseas, prevention is better than cure. Rachel's work has been covered in newspapers, such as the *Sunday Telegraph*, the *Financial Times*, *The Times*, and the *Sunday Express*; and in specialist publications, such as *Energy Day*, *Insurance Day* and *Foreign Policy* magazine. Rachel regularly broadcasts and writes on international security, kidnapping and other aspects of criminal economies.

Doing Business in a Dangerous World:

Corporate personnel security in emerging markets

By Rachel Briggs

The Foreign Policy Centre

First published in 2003 by
The Foreign Policy Centre
The Mezzanine
Elizabeth House
39 York Road
London
SE1 7NQ

Email info@fpc.org.uk
www.fpc.org.uk

ISBN 1-903558-30-1

Cover by David Carroll

Typesetting by Beaufort 5

Doing Business in a Dangerous World: Corporate personnel security in emerging markets

Acknowledgements

I would like to thank the project's Steering Group, who have provided help and support throughout: Baroness Ramsay, who chaired the group; Karl Barclay from HSBC; Mike Basnett and Lloyd Roberts, both from Shell International; David Burrill from BAT; Gary Campkin from the CBI; Graham Fry and Graham Minter, both from the FCO; Noel Philp from Armor Group; John Smith from Prudential; Dr Kathy Sutton from Fellows' Consultancy; Bill Trundley from GSK; Anders Wallin from Group 4 Falck and Eric Westropp from Control Risks Group.

I would like to thank the project's partners, without whose support the research would not have been possible: Armor Group, Control Risks Group, Group 4 Falck, GSK, HSBC and Shell International. Thanks also to BA for providing flights to and from Washington for the fieldwork.

I would like to extend special thanks to all the staff and interns at The Foreign Policy Centre. In particular, to Mark Leonard, Rob Blackhurst, Veena Vasista, Conrad Smewing, Abi Tyler, Laura Vaughan, Matthew Morley, and Daisy Cooper. Thanks to David Carroll for working his magic on the cover design and to John and Michael Breeze for typesetting the text.

Finally, I would like to thank those individuals and organisations who have attended or spoken at project seminars, been interviewed, acted as case studies or have been at the end of the phone for advice. There are too many to thank individually, but their help has been central to the success of this project.

Rachel Briggs, July 2003

Methodological note

The research for this project was carried out over a 16-month period, between March 2002 and June 2003. A number of different research tools and methods were used: a series of seminars were held with expert speakers and attendees examining each of the main areas of the project's work; a large number of people were interviewed and consulted during the course of the research; seven companies were interviewed to act as the case studies outlined; a fieldtrip to Washington to examine OSAC was conducted; and there was extensive desk research.

The case studies used are seven companies that operate in a range of sectors and geographical areas. They are very large multi-nationals and are all companies that have illustrated their commitment to corporate personnel security by their willingness to take part in this study. They are not, therefore, representative of the business community as a whole. They do, though, illustrate the points made. It is also hoped that on a practical level this information will be useful for companies making decisions about staff security.

Introduction

More British companies than ever before are investing in emerging markets, where there are significant opportunities for healthy rewards. But September 11th and subsequent events provided a reminder that these rewards can come at a price: risk and uncertainty, whether at home or abroad.

The risks to staff working in emerging markets are not limited to terrorism – indeed, it is important not to exaggerate the extent to which this crime is a problem. Staff face a spectrum of security risks, from kidnapping, extortion and violent attack to petty street crime and health problems. These risks are caused by political instability, state failings, weak infrastructure, social tension, mass inequalities, under-development and the inadequacy or even absence of the rule of law, characteristics often associated with emerging markets. In the light of the recent war in Iraq and the continuing war on terror and with companies reporting heightened threat levels, it is clear that UK interests overseas may find themselves more susceptible to problems.

It is therefore alarming that the response of the business community has been patchy. Some companies were well prepared before September 11th; for them the events in New York and Washington have brought little change except for perhaps more buy-in from staff. Others note a new interest from their boards, who are now more aware of the threats and are keen to put in place management systems that prevent major loss. But there is still a large proportion of the business community that is doing little or nothing. In a recent survey, less than half of companies had business continuity plans, and only one in ten small- to medium-sized enterprises working in areas of risk were estimated to train their staff.

The report argues that this lack of activity puts lives at risk, and is happening for three reasons.

Firstly, there is a **legal vacuum** around the issue of corporate personnel security overseas. The Health and Safety at Work Act sets out clear guidance on the balance of responsibility between a company and its staff, lays down minimum standards for providing safe working systems and preventing risks to health and safety, educates the workforce to ensure they know what they should be able to expect, and has the means to proactively enforce these standards. That legal framework does not extend to cover security. It is not clear how much further companies should go beyond their health and safety obligations: should they have a responsibility outside the workplace, should this also extend to dependents, what constitutes reasonable care, and is the balance of responsibility between employer and employee different because of the context. This is not something that should be left to the judgment of companies.

Secondly, this is made all the more important because there is **no convincing business case** for corporate personnel security overseas that would ensure companies act regardless of the legal vacuum. Security incidents are a daily occurrence but most are minor and do not represent a serious threat to the company's reputation. While there are efforts within the corporate security profession to quantify the value added to the bottom line, this work is still in its infancy. With the exception of the largest multinationals, especially those working in exposed areas on the ground such as the extractive industry and pharmaceuticals, the business case is weak.

Thirdly, even for those companies keen to act – either through altruistic or self-interested concerns – there is **a lack of publicly available information**. Companies complain that the information available from the UK government is not detailed or business-specific enough to be able to make decisions about security management. While more detailed information is available from private security companies, access is limited by cost considerations, which some companies are reluctant or unable to pay for, and go without. But companies themselves are missing a trick, with few recording anything but the most serious incidents, which means there is poor information on the scale of the problem as it impacts on staff. There is a lack of co-ordination of information available from companies, the UK and other western governments and local governments on the ground. There is also, importantly, little publicly available information on the most effective ways of managing the threat. Security membership and sectoral-based organisations develop standards of best practice among their members, and the companies interviewed as part of this research benchmark against one another on a regular basis. But this activity is restricted to a relatively small number of companies, usually the largest or those sectors that have had their fingers burned in the past because of their exposure. For the uninitiated, there is little information available to get started. Guidance would not only cover the technical management of security. Companies are fast realising that the way they do business in emerging markets can have an important influence on the extent to which they are targeted. Best practice would need to involve guidance for managers right across the business.

This report argues that we need **a new approach to security** to overcome these problems. In the UK, security is characterised by an informality that can breed ineffectiveness or inertia, divisions between the public and private sectors that prevent a comprehensive approach, and secrecy that means there is little visibility or leadership for the issue outside closed circles. It argues for legal reform to put the security of employees on the same footing as health and safety, bringing clarity to employers and employees alike. It also calls for a major push to increase the amount of information available in the public domain and to ensure details are collated from companies and governments to give a better understanding of the impact of security threats on companies and their staff around the world. This type of information will also help to build a stronger business case for companies operating in emerging markets. There must also be much more guidance on what constitutes good or best practice in managing security, both to continue raising standards among those companies that are leading the way and to help smaller companies onto the first rung of the ladder.

This report argues that the UK should aim high and seek to position itself as **the security standard to which other countries aspire**. In recent years the Government has responded to criticism by, for example, improving the content of its travel advice, producing user-friendly formats and introducing new services within embassies. The CBI and the FCO have been in discussions for a number of years about whether and how to improve or change the provision of security information between the Government and companies, and are expected to launch something shortly. All of these initiatives are warmly welcomed. But without an overarching framework that acknowledges the need to overcome the informality, public-private division and secrecy that have blighted effective security, they will not gain the type of momentum needed and progress will be piecemeal.

The Government should launch a **high profile security partnership between the Government and the business community**. This organisation could co-ordinate the services outlined above to meet the needs of both, and research shows there is willingness by both to take part. It would deliver genuine value to public and private sectors and its status would bring the much-needed visibility and leadership lacking in the public management of security. September 11th and the events that have followed are a stark reminder of the vulnerabilities that are now part of our everyday lives. But in their wake there are opportunities for change that will make the UK better placed to cope.

Case study 1

The Role and Management of Corporate Security within the Company

The company organises security on the basis that country and site managers are responsible for the security of their operations. Corporate security is responsible for providing professional and specialist advice, setting policies and guidelines and for conducting surveys and audits. The company has adopted and adapted the DTI and BSI7799 models of the organisation of security. In carrying out their local responsibilities, the company accepts that local laws apply.

Legal Responsibilities

The interviewee accepts that he works within tight legal parameters. He reports that every member of the corporate security team is conscious of the company's legal responsibilities, its corporate governance, ethics and the department's contribution to safeguarding the company's reputation. The company does not draw a distinction between permanent or temporary staff, or even consultants. The company believes that employees must also share responsibility for their own security, and it communicates this through its 'Conduct of Business' handbook that outlines the way the company expects staff to behave while conducting business on its behalf. The corporate security team gets any legal advice they need from within the company and this is gained on a fairly ad hoc basis, especially learning through handling situations.

Personnel Security Policies and Procedures

He reports that staff communication is one of the top priorities within the company. As such, it has evolved a whole range of communication tools. In terms of security, it has a dedicated corporate security site on its intranet. This contains relevant information, such as on-going travel alerts and best practice security management documents. The target audience for this site is everyone in the company, but the most frequent users tend to be corporate security managers, those planning new sites, site security managers and managers, who are dependent on this resource. The site recently launched a comic strip character to get people interested in security, and hits went up dramatically. Besides the website, the company also uses videos and other multi-media, it runs awareness campaigns on all of its sites, security is a component on induction courses, it issues handbooks, the corporate security team regularly contributes articles to the company newsletter, and they conduct security seminars for security managers and country managers in the regions in which they work. Security awareness is one of the criteria on which individuals on the corporate security team are judged.

The corporate security team benchmarks continuously and finds the process very useful. He works through sector-specific groupings and security-specific organisations, such as ASIS and the RSMF. He also notes that benchmarking takes place through OSAC. There is an expectation from senior management that the team should be benchmarking and networking, and security is viewed more often than not as a non-competitive part of the company's activity. The corporate security department is looking for ways of measuring "our ability to be business enablers."

Links with Governments

The interviewee stated that the company does not have contact with the FCO on matters relating to security, mainly because they are an American company, although they do have considerable interests in the UK. He was supportive of the OSAC system and the overall approach of US diplomatic staff, "We would go to the Americans first as they are much quicker and on the ball." He did concede, though, that British diplomatic staff should be well placed to give an excellent service to companies, "…the Brits have a good record of analysing the information and being more objective about it."

7 Doing business in a dangerous world

SECTION ONE:
UNDERSTANDING THE PROBLEM

1 The security risks in emerging markets

The official definition of an emerging market is "A financial market of a developing country, usually a small market with short operating history."[1] The term is also applied more broadly to cover, not just the financial market of these countries, but the country itself. This research project adopts the broader definition, and includes most countries across Asia, Latin America, Africa and Eastern Europe. Of course, security is not an issue restricted to emerging markets. September 11th and the continuing terrorist threat to the West is proof that it matters 'at home', too. Emerging markets, because the risks tend to be higher or different and staff are more dependent on support from the company, are an important starting point where effective personnel security management is most critical.

The opportunities on offer come at a price: risk, and over the last two years perceptions of growing risk have acted as a disincentive for investment. Beyond market volatility and economic uncertainty, companies face a **spectrum of risks**. At one end of the spectrum, there are incidents – both politically and criminally motivated – where staff may be seriously harmed or killed, such as terrorist incidents or violent criminal attacks. The company and its staff may also find itself the target of those with a grudge to bear, such as the local community, political groups such as guerrilla forces, or militant activists. Attacks may range from serious incidents where lives are put at risk to inconvenient disruptions. Foreign companies may also be seen as fair game for extortion in countries where the disparity between the 'haves' and the 'have nots' is stark. Staff can often be the preferred 'easy' corporate target in the face of tight physical security around operations and buildings. Towards the other end of the spectrum, employees face risks generic to all those living in emerging markets, caused by the underlying economic and political instability and weakened rule of law in these countries. They include petty criminal activity, such as mugging and pick pocketing, and health problems, all of which cause some form of harm or loss to the individual. It is difficult to map out a straightforward causal relationship between any individual risk and a particular economic, social, political or cultural factor.

'Managing' these threats should involve companies making decisions about whether or not staff should work in particular areas; if they should, the types of security measures that need to be in place to keep them safe; the types of information and advice about travel and routine that companies need to give to staff to ensure they are able to look after themselves, too; and contingency plans that will enable the company to respond effectively when something goes wrong. In order to be able to make these decisions, companies must balance the probability of something happening with the impact it would have, and their relative vulnerabilities.

Companies not only have to manage the real threats, they must also contend with the perceptions of their staff. Many of the corporate security professionals consulted during the course of this research have observed a growing perception of risk among their workforce. One commented, "There has been a change in perception right from the top of the company down. People are surprisingly attuned to the fact that we live in a new world. I have found that staff want information, are keen to do practices such as evacuations and are more likely to want to make security work." Effective responses to real and perceived threats can be in conflict. For example, while companies might be tempted to put in place very visible security measures to reassure their staff, in countries where anti-western sentiment runs high this may make them a more attractive target for attack. One corporate security manager commented, "One of our local managers was concerned about heightened risk in a particular country and wanted to step up visible security considerably. We took the view that given the conditions on the ground and the level of anti-western sentiment not only would this fail to offer the protection we wanted, it would increase our visibility and make us a more attractive target in an area where we had been working hard to integrate into the local community."

Conversely, many companies complain that they have to contend with staff who underestimate the risks they face and so don't co-operate with security. One of those interviewed said, "We have real problems with men; they don't think they are at risk." Another showed the tragic consequences of underestimating the risks, "We had a man killed in Latin America recently while transferring money in his personal time. We have very clear procedures in place whereby you receive high levels of protection under these types of circumstances, but he had underestimated the risks in what he was doing and had not sought this out." It is therefore vital that companies communicate effectively with their staff to ensure that they understand the threats they face and have access to information about how to behave to limit their risks, but ultimately the decisions of staff will always determine the success of any security policy. As chapter two shows, it is important that there is a clear boundary of responsibility between the company and its staff.

The impact of the risks

It is almost impossible to measure the scale of the problem in terms of the number of workers who fall into danger because figures of this kind are not available. The UK Government collates information, but this is limited to the cases it deals with itself through embassies and high commissions. Not only is this the tip of the iceberg for cases, but business cases are likely to be disproportionately excluded from these figures as those working for companies are less likely to turn to the embassy for help. Almost none of the companies interviewed have comprehensive systems for measuring the scale of the problem they face; they were not able to tell me how many corporate personnel security incidents they have each year. One Corporate Security Director commented, "I suspect more centralised companies have better figures on incidents. I work to a group structure where my role is to advise and recommend, and managing directors for each of our companies takes the lead on security for their own operations. This means that as a group, we have no idea of the number of incidents we have each year, as it is a struggle to get all that information back up the ladder from the extremities. I could probably work out figures for the major cases as the group then tends to get involved, but not the smaller ones." As well as working against particular corporate structures, the localisation of management and the fact that individuals may not be keen to report incidents or see the value in doing so, means that companies do not always have comprehensive data on the extent of the problems they face. This is in contrast to the situation in the UK in relation to health and safety, where the HSE collates comprehensive statistics on workplace incidents.

While it is difficult to measure the direct impacts of the changing risk and security environment beyond patchy statistics and reports from corporate security managers that their workload has increased, there appear to be a number of indirect effects, including on travel and recruitment, the British economy and emerging markets. It is impossible to establish a direct link between these trends and the apparent rise in security threats worldwide. In fact, the trends are likely to be a symptom of this and other factors, such as the increased perception of threats, the global economic slowdown over the past two to three years and the localisation of corporate management.

Travel and recruitment

There is evidence to suggest that real and perceived risks are having an adverse impact on international business. Firstly, there is evidence that companies are reducing their business travel, which may impact on the quality of a company's contacts overseas and its competitiveness in bidding for contracts. Overseas business travel from the UK rose by an average of 7.4 per cent per year between 1997 and 2000.[2] But it is estimated that between 2000 and 2005 business travel will only grow by a *total* of 7.4 per cent over the whole period.[3] The number of trips fell from 8.9 million in 2000 to 8.2 million in 2001, the only recorded annual fall in the last 25 years.[4] And British Airways figures show premium traffic – business and first class – declined 33 per cent year-on-year in September 2001, 36 per cent in October and 25 per cent in November.[5] A March 2002 MORI poll found that nearly one in ten business executives had moved from flying to video conferencing in the previous six months.[6] Although these changes are not due solely to the events of September 11th, the attacks on the World Trade Center and the Pentagon are seen by many as a catalyst for change. The Director of Travel for a multinational company is quoted in an article in the *Guardian* as saying, "For us, business travel has undoubtedly changed more rapidly than it would have done without the events of September 11th."[7]

Some companies are turning away from longer-term postings. In a recent survey, almost half of companies from Europe, the Middle East and Africa said their use of long-term expatriates was declining significantly and just under two thirds were stepping up their reliance on international commuters.[8] These trends are in part due to the fact that staff are increasingly reluctant to travel, especially to areas of the world where they fear the security risks, whether real or perceived. There is also anecdotal evidence that staff are less keen to take up posts in higher-risk countries. One company, for example, found that advertisements for expatriate positions in Damascus, which used to produce half a dozen applicants, did not generate a single response.[9]

Overseas investment

There is also evidence to suggest that overseas investment may be suffering, especially in the developing world. This is bad news for Britain's highly international economy. Net FDI slipped back from a 1999 peak of $179 billion to $143 billion in 2002 after September 11th and the lingering effects of the dot com crash. Of this, an overwhelming $109 billion goes to just ten large countries.[10] Some regions are worse hit than others. Africa's share of all FDI flows to developing economies has fallen from 9 per cent in 1980-85 to 4 per cent in 1996 and just 1 per cent in 2001. Over this period, while FDI to Africa has risen, it has done so much more slowly than regions such as Asia and Latin America. These trends are important for the UK, which is one of the most international of the developed economies. It is the second largest exporter of services, the fifth largest exporter of goods and has the highest ratio of inward and outward investment to gross domestic product (GDP) of any leading economy. British companies are some of the most international in the way they do business. In a 1999 survey of the world's 100 largest trans-national corporations, the proportion of the total workforce of British companies that was foreign was 77.7 per cent as opposed to 56.2 for all companies. British companies had a much higher transnationality index[i] than the group on average: 76.0 per cent versus 52.6 per cent.[11]

The security response by companies

There is a mixed response from the business community to the challenge of keeping staff safe around the world – with worrying numbers of companies that have yet to face up to the challenge. Some companies report having had comprehensive corporate security policies and processes in place for many years. As one Corporate Security Director commented, "Post 9/11 my workload has increased, there is increased demand for our services, more overt demand. But because we already had all this in place this has not created more stress." Some companies are clearly convinced of the importance of security as they are allocating significant budgets for it. An article in the *Economist* in 2000 reported, "In Algeria, where Islamic terrorists trade atrocities with pro-government militias, oil firms typically spend 8-9 per cent of their budgets on security. In Colombia, where leftist guerrillas, pro-government paramilitaries and cocaine barons spread mayhem, the figure is roughly 4-6 per cent."[12] And since September 11th, many commentators have noted the rising interest in security at the highest levels in companies. Writing for *The Unlikely Counter-Terrorists*, John Bray observed, "What's new post-11 September is the increased emphasis on security as a strategic issue. Previously, security was often regarded as a secondary concern that could be sorted out once major investment decisions had already been taken. Now this is

[i] The transnationality index is calulated as the average of three ratios: foreign assets to total assets, foreign sales to total sales and foreign employment to total employment.

less likely to be the case."[13] When asked whether personnel security is a *strategic* concern for their boards, most of those corporate security professionals interviewed thought it was. The case studies give examples of the types of things companies are doing; this includes everything from comprehensive systems to communicate travel risks to staff, and training and awareness campaigns to physical protection and efforts to integrate within the local community.

Some companies were prompted into action by September 11th. In a survey of US CEOs conducted in the last two months of 2001, well over three quarters of respondents were more concerned about the protection of employees after September 11th. As a result, over two thirds had reviewed their business travel policies and a further 11 per cent were planning to do so within 3 months. In a more recent survey of individuals responsible for corporate security in Britain, two-thirds of respondents had seen their security budgets rise since September 11th.[14] This is backed up by a survey carried out by ISMA at the same time, whose members are Global 200 and Fortune 500 companies, which showed that business continuity and personnel safety had been propelled back to the top of the risk management agenda.[15] And one corporate security manager interviewed as part of this research was appointed in the aftermath of September 11th when this position was created. He explains, "I started with a blank sheet. I am hoping to get policies in place over the next few months, but at present we do not have anything formal to refer to." A spokeswoman for the Institute of Travel Management views September 11th as a watershed for companies, "It brought into sharp focus the essential need for everyone responsible for managing business travel to reassess existing travel policies and, of course, to make security a priority."[16]

Other companies opt to transfer their risks through traditional methods such as insurance. It enables them to recoup any financial losses but does little to prevent an incident from happening in the first place. While this may satisfy investors and shareholders that financial returns are secured in the short-term, it will not keep staff safe and it fails to recognise the fact that a company's value is about much more than its balance sheets. Insurance will not protect the company from the threat of litigation should an employee decide to take their case to court. Nor will it prevent negative impacts on the company's reputation, a topic that will be covered in more depth in chapter three. It may be acceptable to manage some assets, such as products, in this way up to a point, but people are special assets and risk management strategies for them must be based on the principle of prevention and deterrence as far as possible.

More worrying is the fact that many companies are doing little or nothing to manage the risks to their staff. In a recent survey of 5000 companies, only 45 per cent had business continuity or consequence management plans in place.[17] One company approached to take part as a case study for this research project declined due to the fact that they do not yet have policies in place. In another survey, employees working for companies from Europe, the Middle East and Africa were twice as concerned as their companies about safety while travelling. There is also evidence that September 11th has brought about regional disparities in attitudes to security. Companies from Europe, the Middle East and Africa in the same survey were six times less concerned about regional safety than their peers in the Americas, where the events of September 11th are likely to have raised awareness.[18] A lack of activity may be due to a variety of reasons. Some companies may be putting short-term business interests ahead of staff security; some may not be aware of the risks they face; and others, of course, may not be working in areas where there are security risks to staff. Given that more companies than ever before are investing in the developing world, the risks of operating are growing, and there is heightened awareness among staff and senior management teams, it is surprising that more companies aren't doing more.

Case study 2

The role and management of corporate security within the company

The Group Security Department is a largish centralised department with a team of regional security managers who exercise functional responsibility with end market security managers about security within their region. The Head of Group Security – the interviewee – reports directly to a board member, the Legal Director. Contact with the board is regular, both routine and on a case-by-case basis during the handling of an incident or a particular piece of policy. There is usually contact most weeks. He reports through audit committees, both centrally and in the regions. "This means the board is taking an on-going interest and sees it as important enough an issue for them to cover. I also have to brief the board formally twice a year." The company's Chairman recently underlined the company's commitment to the safety and security of its people when he spoke about the issue at the AGM. The security team has continual contact with a wide range of departments across the company. The interviewee noted that there has been a rise in the perception and understanding of risk among board members especially over the past couple of years, and claims to have a strong relationship with the board, "I have a most supportive board."

Legal responsibilities

The interviewee felt that staff safety and security comes under a much broader type of responsibility and that this is not necessarily a legal one. "I'm not sure there is a clearly defined legal responsibility as such. There is a duty of care in respect of any employee anywhere in the world." He believes the company is meeting its obligations, "There is an ability to seek advice, people understand how to do this, and there is an ongoing access campaign. Having benchmarked with our peers I don't believe another company delivers a higher level of service." Employees are seen to have an important responsibility for their own safety. This approach is seen as being in line with the overall philosophy or culture of the company, "Everyone knows that security is a responsibility for everyone, both for themselves and for the company. One of our fundamental principles is freedom through responsibility.” He believes the security team has access to all the legal advice it needs. This comes from the legal department, which might also seek expertise from outside the company on particular issues.

Personnel security policies and procedures

Explanation of security policies and procedures begins when an employee joins the company, during the induction process. A security component has also recently been added to the training programme for graduate trainee managers in an effort to ensure that it is integrated into all business decisions. The company has a travel policy whereby those wishing to visit countries deemed to be high risk by the security team must seek permission before they travel. At the centre, all travel bookings should be made through the company’s designated travel agent. When they book, employees receive an email reminding them to seek advice. A similar procedure is followed elsewhere in the world. The principle method of communicating advice is through the company’s intranet site, which also has a link and access to the travel risk database of an external service supplier. While individuals take on this responsibility, there is a trigger for the security team to contact those travelling to high-risk countries if they fail to make contact with them. Where the risks are deemed too high travel is embargoed, and for countries where only business essential travel is permitted the trip must be authorised by the security team and the relevant end market managing director. There is an ongoing awareness campaign, which includes business security workshops each year; one at the centre and one in each of the 5 regions.

The security team has been developing ways of measuring the effectiveness of the work they do and the value added for the company. The interviewee noted, “We have worked out that we get back more than half of the money we spend on security as a measurable before any consideration of qualitative benefits.” Their policies undergo continuing improvement, learning lessons from experience. The website contains a large number of documents that outline best practice and lessons learned from a number of security incidents. They also seek opinions of travellers on security services and information.

The security team regularly benchmarks itself against other companies. This is considered to be a very valuable practice, "Benchmarking is useful in giving a marker. It challenges our ideas and gives us a sense of how cost-effective we are. It is also reassuring to our stakeholders." The company has recently conducted a study involving large multi-national companies from the US, the UK and Europe. They also benchmark through the International Security Management Association (ISMA), which has a database with standards of best practice used by other companies. They have used an external contractor once (for a benchmarking project), and also benchmark internally. They are by their own judgment and that of the other corporate security professionals interviewed, probably the most benchmarked against company.

Links with governments

The corporate security team seeks out links and partnerships with governments wherever the company operates, especially western governments. The interviewee notes in particular that the company draws on UK, US and German Governments. The US is rated as the best government to deal with in relation to security issues overseas. He comments, "The UK is our second choice embassy behind the US embassy. They are useful as a source of quality official information through a process that delivers sensitive information without risk to original source. We get a small benefit from our contact with the UK embassy. We tend to find that their resources are limited and the standard of care is people-dependent rather than organisational-dependent." The divergence in information is welcomed as it assists proper analysis drawing on a range of opinions. It is a requirement for regional and end market security managers to maintain good contacts with local governments and law enforcement agencies on the ground, and these contacts are invaluable.

SECTION TWO: THE CASE FOR ACTION

2 The legal framework

The law in the UK currently falls short of explicitly outlining a company's legal obligations to protect the security of its staff, leaving it open to interpretation by the company. As the case studies and material in the last section show, companies are doing this in a variety of ways, defined by such factors as their corporate 'culture', the extent of buy-in among individuals at the top of the organisation, or the support of local managers. This means that important matters such as the balance of responsibility between the company and the employee and the level of 'reasonable' risk, things that are the foundation of any corporate personnel security policy and management system, are being defined in a wholly subjective manner without check, and often without proper communication of the conclusions to staff. In finding solutions to these problems, health and safety law can be instructive. Of course, security goes beyond the realms of health and safety, which is restricted to the place of work. When employees work overseas they also have to live there and go about their daily lives, sometimes with families present. The extent to which companies should be responsible for staff and their families out of hours, and how they and employees themselves should be expected to deliver their part of the bargain, needs to be clarified, through the parameters of this relationship being more tightly defined.

The legal obligations of companies

All employers have a duty to provide a safe place and safe system of work and to take reasonable care not to expose employees to unnecessary risk. Companies have to do very little to meet this duty of care. In delivering it, employers operating from the UK have a responsibility to carry out and review risk assessments for their staff and operations overseas. They have to demonstrate that they have made reasonable efforts to assess and control risk, and they are not expected to do this perfectly.

The Management of Health and Safety at Work Regulations 1999, Regulation 3, states:

> "Every employer shall make a suitable and sufficient assessment of ... the risks to the health and safety of his employees to which they are exposed whilst they are at work [and of others affected by his undertaking] ... for the purpose of identifying the measures he needs to take to comply with the requirements and provisions imposed upon him by or under the [health and safety at work legislation]. Any assessment ... shall be reviewed by the employer ... if there is reason to suspect it is no longer valid ... or ... there has been a significant change in the matters to which it relates ... and where as a result of any such review changes to an assessment are required, the employer ... shall make them."

And the Health and Safety Executive (HSE) interprets the obligation as follows:

> "The risk assessment provisions ... say that your assessment of risks must be either 'adequate' or 'suitable and sufficient'. These mean the same thing and tell you that you do not have to be overcomplicated. In deciding the amount of effort you put into assessing risks, you have to judge whether the hazards are significant and whether you have them covered by satisfactory precautions so that the risk is small." HSE Guidance, *A Guide to Risk Assessment*, December 1999 (current), page 16.

The Health and Safety at Work Act[19], supported by the Health and Safety Commission (HSC) and the HSE, aims to ensure that risks to people's health and safety from work activities are properly controlled. Health and Safety law seeks to set principles while detailed requirements are covered in codes and guidance to allow the flexibility needed. As the HSC states, since the 1974 law was passed it "has been engaged in progressive reform of the law, seeking to replace detailed industry-specific legislation with a modern approach in which regulations, wherever possible, express goals and general principles and detailed requirements are placed in codes and guidance. Those who depart from the code must be prepared to show that their own approach is an equally valid way of meeting the legal requirements. In this way, flexibility is allowed for technical development, within a framework set by mandatory regulations."[20]

Under common law, a company's duty of care is extra-territorial and so is not limited to within the UK. Individuals who fall into danger overseas can choose whether to sue locally in the country where the incident took place or in the UK. For employees of UK-based companies, the UK tends to be the favoured location for these actions as levels of compensation and health and safety standards are usually higher here than in many emerging countries. Companies cannot easily get out of their potential liability by creating subsidiaries through which local operations are controlled. The key here for English courts is to determine where control rests, and this will differ in each individual case, depending on the management structure of the company and group in question. The only significant way that the employer's overall established liability for negligently causing injury to employees can be reduced is if the employee can be found guilty of contributory negligence.

The case brought against Cape plc is instructive here. In this case, employees were able to pursue their claim in a different country to where the harm had occurred and were able to argue that control – and therefore responsibility – rested not with their immediate employer, but at the top of the corporate tree. Cape was sued by a group of former employees who contracted Asbestosis while working at Cape's asbestos mines in the Northern Cape, South Africa in the 1970s. Although Cape and its London-based largest shareholder the Montpellier Group sold its mines in 1979, lawyers for the South African victims sought permission in July 1999 to take legal action against the company in England. A year later, the House of Lords ruled that such an action could take place. After a protracted court battle incurring legal fees of more than £6 million, a settlement agreement was reached, whereby Cape plc would pay compensation of £21 million.[21] This is also an important case as it establishes the principle of equal standards for local employees as international workers. This is especially important given the increasing localisation of staff and management.

The limits of the law

Working overseas brings risks that cannot be managed solely within a health and safety framework because they concern the safety and security of people *outside* the workplace. The law is not clear about the extent to which a company should take responsibility for the employee at their home, on their journey to and from work or even during their leisure time. There are a series of other questions that remain unanswered:

Who are companies responsible for?

Work and employment patterns have changed significantly in recent years. There has been an increase in using sub-contractors over permanent staff; there has been a localisation of the workforce; there are also more temporary workers used. In the light of this, what is the extent of a company's duty of care? Companies consulted during the course of this research claim to take a responsible and inclusive approach. One interviewee said, "We don't draw a distinction between permanent staff, temporary staff or even consultants. We take the view that if they are working with us then we have a responsibility to them, regardless of what the law says. We take this line to both keep our people safe, but also because we recognise the reputational implications of not doing so." This question became a live one for BT when one of its sub-contractors was kidnapped and subsequently killed while working in Chechnya. At the time, there were accusations that BT had operated a two-tier system, extending less support to this man than it would have done to a permanent employee.[22] There is also confusion about whether responsibility should extend beyond the employee to their family and dependents in country. Many companies consulted claim to adopt this wider definition of duty of care, with one commenting in a research seminar that involving the family in briefings can in fact strengthen their impact and thereby enhance safety and security. This anecdotal piece of evidence is backed up by a study of BG workers in Sao Paulo and Cairo that found that employees who have family with them while they work overseas are more likely to take an interest in security.

While the Cape plc case illustrates the need for parity between local and international staff in relation to health and safety, some companies admit having to wrestle with this in handling security. Firstly, locals are not unfamiliar with the risks, although in some cases they may find themselves exposed to threats they ordinarily wouldn't be due to the identity of their employer. Secondly, there are practical issues, such as whether a company can demand the evacuation of workers from their home country in the way that they would be more able to do for international staff.

What is the balance between company and employee responsibility?

The Health and Safety at Work Act, while limited to health and safety and within the UK, is important within the context of security overseas as it defines the nature of the relationship between employer and employee. Importantly, it enshrines the principle of shared responsibility. The HSC states, "The starting point and main principle of the Health and Safety at Work Act is that it is those who create risk from work activity who are responsible for the protection of workers and the public from any consequences." As well as there being an ethical case for individuals to take on a certain amount of responsibility, there is also a practical one. The way in which corporate personnel security policies are applied will determine their effectiveness, and the decisions and behaviour of those being protected are a limiting factor.

When working in emerging markets, though, this balance must shift further towards the company. This is firstly due to the imbalance in knowledge between the company and the employee, which leaves the individual less able to make decisions about their safety than they would in their home environment. One of those interviewed commented, “When people go overseas they find themselves in different and difficult situations so there is more onus on the company.” Arriving in a new country, employees often find it difficult to read the danger signs that enable them to predict problems arising and stay out of trouble. Researching the effects of the social and physical environment on expatriates in West Africa, Wicker and August showed that recognition of cultural differences is one of the key defences to staying safe. They call this an individual’s ‘sense-making’ cycles, “…people as they go about their daily lives are exposed to a vast array of events…the particular environmental events that they notice depend on their existing ‘cause-map’, their prior understandings about the world.” This explains why even employees who live in cities with higher crime rates in the UK than their posting can fall victim to local street crimes because they are unable to read the signs as they would have done at home.[23] Travel advice can help by providing information that allows individuals to create their new sense-making cycles: instinct is a tool to be exploited, but it needs to be pre-programmed.[24] Companies can help by ensuring employees have sufficient time to settle in and language skills to allow them to integrate themselves.

Secondly, the actions and behaviour of the company will have an influence on the individual’s ability to stay safe. A company’s culture is perhaps the most important factor influencing the extent to which its staff will be kept safe. Companies need to develop ‘pro-security’ cultures, where security is considered integral to the running of the business, rather than something that gets in the way of business priorities. Those companies that adopt this culture are likely to go beyond their legal obligations in delivering security for their staff. A company’s culture will also determine the extent to which employees feel comfortable discussing their worries and fears with colleagues or managers. Individuals require help and support from their employer, but may avoid asking in a company that does not take security seriously. There are numerous examples of companies that have suffered security threats as a consequence of either their security policies or their general operational behaviour.[25] A company with a pro-security culture is more likely to take a broader view on security, and appreciate the connections between their company's behaviour and their long-term security needs and therefore, ultimately, the sustainability of investment opportunities in a given region or country.

There is much discussion within the corporate security community about how this culture can be encouraged. Corporate culture is, after all, a product of the policies, practices and attitudes of leaders with a company. As well as changing the detail of personnel policies, one other possible solution would be to have security representation at board level, or at least to ensure that the corporate security manager – if there is one – reports as directly as possible to their board. This would help to promote the profile of security within the organisation. One of the companies interviewed has added a security component onto their company's management training programme for fast-streamers. This is motivated by a desire to make security a concern across the company outside the corporate security department, thus becoming an integral factor in all company decision-making.

Security briefings and travel advice can equip individuals with the information they need to make everyday decisions that help them avoid danger. But the value of this information is limited if it fails to reach its intended audience, or if the individual does not then act upon it. The key here is ensuring that employees have an accurate perception of the risks they face and the fact that advice can help them to avoid these threats.[26] Companies must examine the methods and channels they use to communicate with staff, and the content and detail of the advice they issue. There is limited value in setting up a website, as all the case study companies have done, unless there are regular and direct prompts for individuals to visit it or have the information delivered directly to them. They must also avoid information overload that causes employees to switch off from all advice.

There is also evidence to show that individuals respond much more positively to advice when they are able to see the direct relevance to themselves. Dr Jim Alvarez, a psychologist who works with many multi-national companies on these and related issues, comments, "You need to answer the question – what does it mean to me? Why do I care about this?"[27] In the previously quoted BG study in Sao Paulo and Cairo, a large proportion of respondents described the briefings they received on the ground as some of the most useful. It states, "In-country security briefing and the sharing of security information between colleagues and friends outside the company were rated high by the respondents as effective sources of information."[28] Some security managers have commented that they find it useful to organise briefing sessions for staff in country where they are able to listen to those who have experienced security incidents first-hand and apply these lessons to their own lives in the same location. These messages are much more credible than dry communiqués from head office.

There is also a tension between the company's responsibility to do what it reasonably can and an individual's right to freedom of action. This challenge is highlighted by a recent example cited by one company in the Middle East during the build up to the war in Iraq. It had deemed that the risks in a particular country had become too high to justify them staying, but one international member of staff refused to leave. They could not force him to go, but felt a sense of responsibility for him and were unsure about their liabilities. At the time, one of the corporate security team confided, "We are confused as to what to do. We're not sure where we stand legally."

*What constitutes **reasonable** care?*

Perhaps the most important role played by the Health and Safety at Work Act is setting a benchmark of what constitutes *reasonable* care on the part of the employer, something which has not been done systematically in relation to security because of the legal vacuum. It is of course impossible to eliminate all risks from the workplace, or anywhere else for that matter. And while it may be possible to eliminate some, the cost of doing so may be disproportionate to the level of the risk or its potential impact. But leaving this judgment entirely to companies, as is currently the case, is not in the public interest because of the obvious conflicts of interest. The HSC and HSE acknowledge this by describing 'reasonably practicable' as being where the duty holder takes precautions "up to the point where the taking of further measures would be grossly disproportionate to any residual risk." The guidance issued by these bodies then defines what this means in relation to a wide range of risks in the workplace.

Does the law force companies to act?

The law does not currently provide the push needed to make irresponsible companies act because cases are so rare. Firstly, because there are relatively few serious cases, which are also spread across a number of countries, companies could be forgiven for assuming it won't happen to them. Secondly, even when an incident occurs, individuals and their families are often keener to get on with their lives than relive a traumatic experience in a courtroom. And when cases do reach court, the incentive for both sides is to settle quickly out of court, and costs can often be written off across the business.

The 1999 Turnbull Report on Internal Control has brought a certain rise in accountability by requiring companies listed on the London Stock Exchange to issue annual statements defining their policy on all aspects of risk management, including security. Similar requirements apply in other jurisdictions, such as under Germany's *Kontrag* regulations. This means that companies must document whether they are managing risks and this information could be useful in the event of a problem. The case of Union Texas Petroleum shows the value for companies of having proper systems in place and documenting what they do. The company was issued with a $100 million lawsuit by the families of four Americans who were murdered during a trip to Karachi, Pakistan to carry out an audit. The company won the case because they were able to show documentation that the individuals concerned had been briefed prior to departure, the company had used a variety of sources of information and it had not contradicted the US government's advice. The judge concluded that they had undertaken everything that could be reasonably expected.

The health and safety policy framework is not without critics. Some argue that it does not go far enough. Trades unions continue to campaign for the HSC and HSE to be tougher on companies. On the other hand, some argue that health and safety law has gone too far and has created what might be termed 'nanny corporations', where companies are responsible for reminding employees about dangers that should be common sense. It is of course important to get the balance of responsibilities correct. But it cannot be denied that the legal and policy framework on health and safety in the workplace has helped to bring about cultural change within companies that has transformed the workplace and made staff much safer. Between 1986/7 and 2000/1 the number of injuries over 3 days per 100,000 fell by a third and in the same period the number of fatal injuries fell by over half.[ii] There is clearly much to be learned from this system of managing risk that could be applied to corporate personnel security overseas.

[ii] These figures are those cases for all industries reported to all enforcing authorities by industry, and do not cover the self-employed. The full data set can be found at: www.hse.gov.uk/statistics/xl/histrate/xls

Case study 3

The role and management of corporate security within the company

The interviewee, who is the Director of Security for the company, reports to the Director of Human Resources who is not a member of the main board, but sits on the Executive Council. Contact with the board is on the basis of unimpeded direct contact between the Security Director and the relevant Executive Director(s) as the Security Director deems necessary. For example, in the run up to the recent war in Iraq the Security Director submitted the department's strategy on security contingencies to the Executive Council for their official approval. The interviewee comments, "I prefer to let the board get on with what they are good at [meaning strategic matters] and the security department is trusted to get on with its own job." Responding to a prompt about regular formal contact with "the Board" in the build up to the war, "I don't feel this is necessary generally, but in a critical situation I tend to get more formal." Contact with other departments is on an "as necessary basis, from the Chief Executive to the people on the ground."

Legal responsibilities

The security team is not versed in legal intricacies. Instead, it starts from the assumption of having a duty of care for staff and interprets this as doing what they understand to be reasonable and comparing that with what others are doing. The interviewee notes that the company does not differentiate between staff and temporary contractors. He comments, "We treat sub-contractors as if they are our own staff because we recognise that we are the bigger presence and tend to call the tune. We also do this with our junior partners. I'm not sure what the legal implications are of doing this, but with the speed of events recently it seemed like the right thing to do. Our approach is one of getting the job done and arguing about the costs later." When they need to, they take advice from their legal department, but this tends to be in response to unfolding events rather than the legal team having any input when security policies are being drafted.

The interviewee believes there is no confusion about their legal responsibilities, "The security function is quite strong and reasonably well regarded, and we haven't had disputes beyond the occasional bleat." He notes the importance of employees taking a degree of responsibility for their own safety. The company offers general advice and communicates with its staff what their own responsibilities are. He commented, "You get to the point where individuals have to take a degree of responsibility."

Personnel security policies and procedures

The company has a travel policy that enables corporate security to monitor the movements of staff and ensure information is available about the risks they face and how best to manage them. All travel is routinely booked through a central travel company, which is blocked by security from issuing tickets for countries designated as high risk by the company without the travel request being assessed by security. Flexibility is an important characteristic of the system, though, and in some cases there is leeway. "After the Bali bomb [in October 2002] two employees needed to go to Indonesia while there was a corporate ban on travel to the country. We contacted the men, who had been there before, knew the area well and were experienced travellers. Because of their experience and knowledge, and our existing in-country infrastructure, we deemed it was an acceptable risk for them to travel. On the other hand, following September 11th we had a guy wanting to go to Egypt. Because he was an inexperienced traveller who didn't know the area at all, and the trip was not business-critical, authorisation was not given for the trip." He reports widespread support from staff for the work they do, "When we issue warnings many people are relieved as they don't have to make the decision themselves. They tend to be understanding, as long as we are clear about how we have come to our conclusions." The main method of communication is the company's intranet site, which has a dedicated site for corporate security. There are hotlinks to the FCO, the State Department, the Australian Government's travel advice service and staff are able to access the travel risk database of Control Risks Group. The focus is on giving staff the information they need to empower them to draw their own conclusions based on best available information. "They can compare advice and challenge it, and this is a fruitful way of reaching decisions."

The corporate security department regularly takes part in formal benchmarking exercises against other companies in their sector, chosen on the basis of common interests and concerns. They also benchmark informally on a day-to-day basis through organisations, such as ISMA, that have useful information and peers in other companies either in the same sector or working in the same parts of the world. He is unconvinced of the value of formal benchmarking on an expanded scale, "There are some companies that make decisions for the wrong reasons. For example, I recently heard about a company taking people out of a particular country due to the personal concerns of a senior individual, despite the better judgments of others within the company. I want to preserve the authority to make our own decisions and set our own standards in relation to whom we benchmark against. In that way we would not inadvertently become hostage to a set of decisions with which we might deeply disagree, but which it would be difficult to appear to ignore if we had 'signed up' to some sort of benchmarking club".

Links with governments

The company has good links with the FCO, mainly on an informal footing. He notes, "If I have a specific concern I might go through an informal contact. Our Chairman interacts at a very senior level with the FCO." On the formal side, there was frustration at the type of information available for companies and the limitations of generic advice for all travellers. "I feel the FCO needs to differentiate between tourists and those living and working overseas. After the Bali bombing, definitions of 'essential' [presence in country] became stretched". He reports that the company maintains good contacts directly with embassies in almost all of the countries in which it operates, and claims this adds significant value to its work. He tends to find the attitudes of staff in embassies are positive and forthcoming, "They tend to be honest. They often comment off-the-record, but this is still useful. We know how to get hold of the right people if we have a problem." The company also takes information and advice from a range of other western governments, including the US and Australia.

3 The business case

There is a business case to be made for companies to look after the safety and security of their staff in emerging markets, but it is stronger for some companies than others and it is not compelling enough to make all companies act without legal reform. Corporate security managers struggle to quantify the value their departments add to the business or the amount of money their services save in the long-term, but despite this many companies are investing significant amounts. This is because the business case is about much more than profit and loss; it involves a series of complex relationships around the way the company operates, its reputation among its stakeholders and the knock-on impact on future performance. However, while reputation, recruitment, retention and so forth are boardroom concerns and while increasing numbers of companies seemingly convert to socially responsible business activity, the extent to which the management of corporate personnel security is an important factor will differ from company to company and sector to sector.

Reputation and business performance

The importance of reputation is not lost on boards. Companies with a strong and positive reputation tend to do better; those on the *Fortune* 'Most Admired Companies' index consistently outperform the market average. They are also more likely to find it easier to operate: regulators may look on them favorably when granting licences; local authorities may take it into account when dealing with planning applications; financial markets are more likely to raise capital for companies with good standing in the marketplace; and entry costs into new markets can be reduced, thereby securing a price advantage.[29] There is also evidence to suggest that a poor reputation can impact on a company's ability to recruit and retain the best people, which can be a severe limiting factor on performance. For example, the Brent Spa incident did not affect Shell's bottom line, with profits for 1995 at a record high. However, the company admits that its ability to attract the top talent dipped and this had a significant effect. The importance of this for most companies is unclear, particularly given the increasing localisation of workforces.

A recent report from the Institute of Business Ethics offers proof that there is a link between the best-managed companies, those with a stated ethical policy and the highest performing companies. Using four indicators of business success – economic value-added, market value-added, price/earnings ratio volatility, and return on capital employed – it compared two groups of companies: those with a demonstrable commitment to ethical behaviour through having a published code of business ethics, and those without. Their performances were then analysed over the five years 1997-2001. On all of the indicators except return on capital employed where the results were less clear, the companies with codes were clearly superior.[30]

The link to personnel security?

The extent to which reputation can be part of a business case depends on how important an influence corporate personnel security can have on it, and this seems to differ between companies. The case against Union Texas Petroleum shows incidents of corporate personnel security can impact on reputation. Although the company won the case, they did suffer. As a recent report by Armor Group concludes, "The company won the case, but it illustrates the legal and reputational jeopardy which companies face through their deployment of staff overseas."[31] The probability of experiencing a major people security incident is much higher for companies who work in the areas of highest risk or who have employees working in exposed areas where it is harder to offer protection. It is therefore no surprise that extractive and tobacco companies are at the forefront of security discussions, and are viewed by their peers as having some of the most effective security management systems. These companies have also often learned the hard way through experience. On the whole, it is likely to be more important for larger companies than smaller ones. They have a wider coverage on the ground and their size also gives them the benefit of economies of scale in managing their security risks. They also tend to be more sensitive to reputation damage because they have more to lose. There is also a lot more interest in their behaviour from non-governmental organisations (NGOs), activists and the media. There are obviously exceptions to this rule. For example, some small companies work under risks that larger companies could not tolerate and use this flexibility as their unique selling point on contracts.

An important study by Oxford Metrica could also be presented as more evidence of the value of taking personnel security seriously, as it shows that not only do the best-prepared companies tend to fare better in the event of a corporate crisis, but some actually came out of it financially better off than they were before. This appears to be due to the scrutiny that management systems and capabilities receive during a crisis that they wouldn't otherwise. Confidence can be strengthened if senior management can be seen to be doing a good job. With security threats rising in many parts of the world, it is important that companies have effective policies and procedures in place both to avoid the problem in the first place, but also to ensure that should the worse happen they are able to respond effectively.[32]

However, the extent to which the link between corporate crisis and reputation is applicable to personnel security is questionable. The cases examined in the study are examples of true corporate crisis – i.e. where the ability of the company to conduct its business is challenged by an incident. For example, the 2000 Air France Concorde crash, the 1999 Coca Cola health scare and product recall in Belgium, and the 1994 discovery of a flaw in Intel's Pentium microprocessor. Only the most extreme personnel security incidents, such as kidnaps or murders, might fall into this category, with the majority of cases not even hitting the radar screens of corporate security managers interviewed.

A Broader Case?

The business case for security also works in reverse, i.e. the way a company conducts itself, regardless of its security measures, can impact on its security within a local environment. A good example is that of International Water in Bolivia, which led a consortium for a multimillion-dollar electricity and drinking water network. After water supply was privatised by the Bolivian government rates rose by 35 per cent, putting drinking water out of the reach of a large proportion of the local population. A 'water conflict' followed lasting ten months, causing huge economic losses, the declaration of a national state of emergency and several deaths. Throughout, the company was targeted by locals venting their anger at its behaviour.

Companies also, of course, have an interest in the long-term sustainability of the markets in which they operate, with security being one of the most important limiting factors in emerging markets. It is not surprising that many companies are not only conscious of how their business activity impacts locally, but are going further by spearheading initiatives to tackle the causes of instability. For example, in 1995 Business South Africa, an umbrella organisation for all the country's chambers of commerce, launched 'Business Against Crime'. The aim of the programme was to leverage resources from businesses and the local community to support the government in reducing crime to the level at which the country could have a successful standing in the world economy. Between 1995-98 in Gauteng Province alone, its achievements included establishing two anti-hijack reaction field team units that recovered over R15 million in stolen property; establishing a victim support programme in 45 police stations that reached approximately 160,000 people; setting up support partnerships involving local companies in 53 police stations in the province; two of the region's most strategic police stations were refurbished with business support; CCTV was implemented in the central business district of Johannesburg; a crime information centre was set up; over 300 members of the South African Police Service were trained in management skills through the Joint Universities Public Management Education Trust; and the Youth Against Crime initiative was inaugurated in schools.

Without a strong traditional business case to take corporate personnel security seriously, though, it is unrealistic to expect most companies to act voluntarily. Even though numerous business cases have been made for so-called 'corporate social responsibility', progress remains slow with the usual suspects sitting around the table talking to one another. Milton Friedman said, "There is only one social responsibility of business – to use its resources to engage in activities to increase its profits so long as it stays within the rules of the game." The problem as far as people security in emerging markets is concerned is that there are no rules. This section has shown that the legal and policy framework needs to be strengthened and that health and safety might provide a useful model.

Case study 4

The role and management of corporate security within the company

The interviewee, Head of Group Security, reports to the Group Chief Operating Officer. He is sometimes required to report to the Group Audit Committee, which meets quarterly. This would take the format of either a short paper or a question and answer session. “For example, I went along before the war in Iraq with no paperwork; I spoke for five minutes on the threat, the measures we were taking and answered their questions.” The Group Audit Committee gives feedback to the Group Chairman. He has the freedom, though, to operate informally within the company on any level, right to the top, through one-to-one contact. “The company likes doing business one-to-one rather than through committees.” He has contact as and when it is necessary with individuals on the board, including the Group Chairman, the CEO, the Finance Director, the UK Chief Executive, and Chief Executives overseas on holdings boards. He reports a good level of support, “The Group Chief Executive is very supportive in making resources available for protecting people, without questions being asked.”

The role of corporate security seems to be slightly unclear and because of the shape of the organisation most of the decisions are decentralised to the lowest levels, with corporate security responsible for creating resources for local managers to use and handling the most serious incidents. As the section below on policy will show, this could impact on the ability of the group to co-ordinate an effective corporate security policy for people overseas.

The corporate security department has good relations with a range of other departments, especially administration, property, legal, compliance, human resources, IT security and internal audit. Those relationships also apply through subsidiaries, too. “We have to be seen to be part of the business rather than something that looks in from the outside.”

Legal responsibilities

The interviewee claims that all staff, permanent and temporary, are treated the same in relation to corporate personnel security overseas. There is a very strong emphasis on the responsibility of individuals, with the company's role being one of support, "The ethos of the company is that it is up to everyone to look after security but that they need help to support them, but not to nanny them. Some companies go to great lengths to tell people what to do and what not to do. It's not like that here. We tend to be the first in and the last out. There is an understanding that we have to look after our staff but there needs to be a reliance on people to get the job done. We expect individuals to be proactive in looking after themselves. All of these things are unsaid." He did not believe there is any confusion about where the responsibility for duty of care lies – with local managers – because the lines of responsibility are clearly defined within the company.

Personnel security policies and procedures

The company's security and travel policies are at a very early stage of development. The interviewee has been in the post – a new role – for under a year. "If you ask me these questions again in a year's time you might get a different response. I have started out with a blank sheet and it's still very early days in development." In many countries there is no permanent security manager, but recruitment is a priority. He has recently launched weekly information and risk bulletins and the travel security policy has been in place since March 2003. The team produces general handouts for all people who book tickets and those travelling to higher risk countries receive a verbal briefing. There is also a handout for staff living overseas.

There is currently no global security section on the company's intranet site, but this is planned for the near future. "I am very impressed with the World Bank website, which is comprehensive without being difficult to read. It gives you everything you need to implement security without speaking to a security manager. It gives contingency plans, procedures, instructions and so forth. I intend to model our site on their's." The target audience for the site is therefore middle management rather than travelling staff.

There is no central knowledge of what goes on within the businesses across the world. This is not a priority for the foreseeable future as, in the absence of security functions in many parts of the world there would be no natural point of contact for reporting incidents. The interviewee admits, "I have no idea how many people security incidents we have. I could work out the major incidents, but not the smaller ones. We don't have the reporting structure in place yet."

The corporate security team benchmarks against other companies on a regular basis, mostly informally. "We are benchmarking, but not in a systematic way." One of the organisations used for this purpose is ISMA, which issues standards that are relevant for people security. But the results of these studies need to be interpreted with care to meet the specific needs of the company, "I am keen that we do not base what we do on what other people are doing; we need to adapt to our own needs determined by where we are geographically and what the threat levels are."

Links with governments

The corporate security department does not have much contact with the FCO, and what it does have tends to be through personal contacts. The interviewee has contact with a number of western governments and believes the UK lags behind, "The US Government is much happier to sit down with business and let their analysts talk about things. The UK Government is badly wanting in this regard. Many parts of government want to help business but don't know how to do it. I have had help in the States in a way that wouldn't have been possible in the UK without having been in the public service. I have had very good contact with the French, too. I have had a lot of co-operation." Each company overseas tends to keep in touch with embassies on the ground, as do the heads of security, and they take part in the warden service in certain places.

The company does not have sufficient contacts with governments on the ground. He notes, "I want my staff to have more contact. I have recently posted someone to the Middle East and instructed them to talk to the police, security services, and so forth. So far, they have been very well received. These types of contacts are increasing and this is a reflection of a changing ethos which is being far more proactive than ever before."

SECTION THREE: THE TOOLS FOR CORPORATE PERSONNEL SECURITY

4 Information needs

There is a lack of suitable publicly available and free information on the security risks facing companies and their staff working in emerging markets. Companies claim FCO travel advice is not comprehensive enough and falls well short of meeting their needs. It is also not practical enough to give staff the information they need about both the risks and also what they should be able to expect from their employers. Unsurprisingly, there has been a surge in the number of companies offering such services to the business community – but at a price. This excludes companies that can't afford to pay – precisely those most in need of all the support they can get – as well as individual employees. There is also concern within the business community that it is impossible to guarantee the quality of these private services, and some of the companies consulted during the course of the research expressed a willingness to pay for more detailed government information and services.

The information needs of companies

Companies need information for use in making decisions about security management and staff deployment. In a seminar, held as part of this research project, a group of corporate security managers defined their basic information needs and divided them into two categories.

First, companies need **information about the broad security environment** in which they operate. A number of factors may trigger threats to the safety of their personnel: politics, terrorism, crime and organised crime, reputation issues, travel risk, the capability of local law enforcement and military forces, bribery and corruption, and militant activism. Wherever possible, briefings should include information specific to a given country, region, business sector or individual company. This information helps to give companies a clearer picture of what risks their staff might be exposed to. It also allows them to make basic decisions about project development, whether or not and how to deploy staff to a given locality and when to evacuate staff from the country or region in the event of a major problem. Second, companies would also benefit from **information on security contacts overseas**: local consultants, local security providers, introductions to local law enforcement and the identity of a person acting within the embassy as a focal point for all information and services.

Government information and advice

The UK Government's FCO provides information and advice on travel safety and security, accessible via its website, telephone, fax, and Ceefax. The service includes information on the political context on the ground to give a broad overview and introduction to the country; the main security risks, which might include anything from terrorist attack to bag snatching; health risks, such as malaria or advice not to drink tap water; through to the practicalities of getting around, such as road regulations or local customs. The FCO's audience for this advice is the whole of the travelling public, which amounted to 66 million trips in 2002 and covers everyone from package holiday-makers heading for the Costa del Sol and backpackers on their way to Peru to business workers, aid workers and Britons living overseas permanently. All corporate security managers consulted during the course of this research agree that it provides them with neither the right type of information nor detailed enough information to meet their needs. One commented, "The FCO needs to differentiate between tourists and those living and working overseas. After the Bali bombing definitions of 'essential' became stretched." At the time of the Bali bombing an ISMA survey found that only 2 of 55 companies questioned were removing their expatriates from Indonesia in line with warnings. This is backed up by research for the report, *Travel Advice: Getting information to those who need it* which showed that different types of travellers and organisations need different types of information and recommended that the Government should offer more specialised services.

The government is rightly wary of accusations of offering advice selectively or better advice to some groups than others. A memorandum submitted by the FCO to the Foreign Affairs Select Committee on 31st January 2003 picks up this point: "We need to be careful about accusations of picking and choosing between groups; and of implicitly offering a better service to some." This, however, ignores the fact that different groups have varying needs as well as the fact that greater information is already handed out on an informal basis. Firstly, giving information about all risks to all travellers may actually result in confusion rather than better preparedness, as it is difficult for the individual to work out which warnings apply to them. There is also no reason why business-specific information could not be accessible to all but actively disseminated only to those who sign up to a delivery service or who use a particular web site. What we need is better travel advice for all, and this means tailoring it to the needs of individual groups. Secondly, some in the business community claim to get access to more detailed information through personal contacts, especially those who have previously worked within government or other public services. This comes out in the case studies, and a different security professional commented, "Relying on a friend of a friend or the 'old pals act' seems less than professional in today's world".

The FCO's network of embassies, high commissions and consulates gives it a presence in almost every country in the world. Posts already do a considerable amount of work for British companies to help them trade, invest and do business on the ground, including the work of British Trade International. Staff are also available to offer some help to companies in relation to corporate security, but this is not systematic, reports from companies are mixed and it tends to be poorly advertised. Companies have both good and bad stories about embassies. They report a lack of consistency, "We tend to find that their resources are limited and the standard of care is people-dependent rather than organisation-dependent." Another comments, "We would go to the Americans first as they are much quicker and on the ball. I don't bother with UK embassies." There is a sense that staff within embassies are not interested in working with the business community, "In Britain, unlike the USA or our European neighbours, the view seems to be that business is a dirty word. There is an elitism, which may be disappearing, that gives the impression that they don't want to deal with commerce." Coming from some of the country's largest companies, this is not encouraging. But companies consulted were complimentary about the standard of analysis from FCO personnel and tended to find the pragmatic approach of the British far more compatible with the demands of doing business than that adopted by some other governments.

The negative feedback is largely due to the fact that the FCO does not have comprehensive policies and procedures defining how embassies should work with the business community on matters relating to corporate security. In some ways this is sensible as in theory it allows posts to develop the most appropriate services for the local situation. In practice, it can get in the way of progress as all initiatives require the personal energy and commitment of local staff – one of the problems for companies too highlighted by the case studies – who may also find themselves reinventing the wheel every few years with the turnover of people. It is important that the business community understands exactly what it should be able to expect from the UK Government and its posts around the world. Where any service is being delivered, it is vital that the intended target audience understands what is available and how they can get it. A certain level of service provision should be universal, with each post having the flexibility to respond to specific needs as they present themselves on the ground.

Companies often struggle to make contacts overseas. British embassies already make introductions in relation to trade, though not usually on security matters. This does not have to involve them recommending one security supplier over another, something which the embassy would naturally be keen to avoid. But just as the embassy has other lists of suppliers and contacts relevant for exporting and investing, security lists would prevent the duplication of work to establish what is available and where.

The CBI and the FCO have been in discussion for a number of years on the possibility of making services relating to corporate security more consistent between posts. It is expected that an initiative will be launched shortly that will outline the responsibilities of posts and require them to be more proactive. This move is extremely positive, but without full details of the scheme it is impossible to know whether or not it will address the full range of problems identified within this report.

Private security companies

The information gap in part explains the considerable growth in recent years of private companies offering business-specific information and security consultancy capabilities. Companies such as Control Risks Group, Armor Group, The Risk Advisory Group, Janusian and Kroll offer a range of services, from travel risk databases and warning systems that many of those interviewed claimed to use, to detailed analysis work on the security risks for a new project or horizon scanning. While this provides a partial solution for some companies, it excludes those that cannot afford the commercial prices or those that see security as a low priority. As one security expert noted, "Currently the high cost of gaining this sort of information is prohibitive. Most small to medium-sized companies go without." According to Cigna Property and Casualty, only about one in ten middle-market companies exposed to overseas risks provides formal training aimed at reducing vulnerability to violence and crime.[33] There is also no guarantee of quality, an issue raised by a number of those interviewed. One commented on the use of private companies in audits, "We don't use private security companies as we find the quality varies. You tend to find that your point of contact is not the person who goes out to do the work and we have had bad experiences in the past."

It is vital that companies, regardless of size, budget or experience, have access to at least the basic level of information they need to manage the security risks to their staff properly. Given that the FCO is processing much of this information anyway, has a network of embassies on the ground and has a self-defined aim to promote the competitiveness of the British business community in global markets it would seem sensible for it to co-ordinate such a service. Furthermore, some corporate security managers consulted during the course of this research claimed they would be willing to pay for such a service.

The information needs of employees

It is also important that employees have access to a publicly available source of information about security threats so they do not have to rely on the information provided by their company, which may be open to accusations of corporate bias. Firstly, they need information about the risks they face so they can make informed judgments about where they work and therefore only ever take risks knowingly. Secondly, they need advice about what they can do to make themselves less vulnerable, which should be as practical and focused on their needs as possible. As discussed in chapter two, as well as public sources of information, there is also a need for companies to play a role. On occasions there may be conflicts between these sources. For example, where publicly available information applies to a country as a whole and warns of generic risk, but a company is able to analyse more detailed information that also takes account of their exact location and the specific protection measures and procedures adopted to reduce the risks. Thirdly, employees also need to know what they should reasonably be able to expect from their company so they can apply pressure from within. This has been an important feature of the work of the HSC and HSE in the UK, part of whose aims is public education. Much of this is done indirectly through trades unions, but they also contribute to wider dissemination. This provides support for individuals who may feel uncomfortable raising concerns without knowing for certain whether their claim is legitimate. A similar function is needed for security overseas.

Case study 5

The role and management of corporate security within the company

The corporate security function sits at the corporate level as a service organisation. Separate security policies are run at the individual company level, with the centre setting a 'standard' rather than detailed policies. Security is often linked into health and safety. The security standard is enshrined in the company's governance process, with country managers required to sign a letter of compliance of these principles as part of the annual assurance process. The company is run by a board, but corporate security seldom has direct contact with this body, working instead to a senior director in the corporate centre. Where there is contact, it would usually be related to a risk to one of the board members personally. The interviewee believes the board is committed to corporate personnel security and sees it as a strategic issue in the company. The Chair of the board outlined the company's commitment to it in a recent message to staff. Contact is as required with other service organisations and the different business units. The security team's most frequent contact is with their senior director in the corporate centre, public affairs, businesses and the individual operating companies to which they provide services.

Legal responsibilities

The company defines its legal responsibilities in its Business Principles. Responsibility is devolved down to the lowest possible level, usually resting with line managers and country managers. Line managers are expected to check that their employees understand the business principles. Everyone has recourse to the legal department should they need it, and the interviewee believes he has all the information he needs. An onus of responsibility is also put on the individual traveller. Information on security risks is available, co-ordinated by the security department, but staff are reminded by their travel services to seek it out themselves.

Personnel security policies and procedures

The main method of communicating travel risks is through the company's intranet site, which contains various pages on different elements of travel. The security homepage includes links to websites of the relevant governments. It also directs the visitor to the websites of individual operating units and the site has its own travel warnings. The emphasis is on having as many different sources of information as possible, including news sites, such as CNN and the BBC. The website also contains practical documents and is used as a means for sharing lessons learned. The central corporate security team runs regular workshops and occasional meetings, both in its head offices and around the world.

All travel should be booked through the designated company travel agent. For those countries which the company deems are too high risk, either in the short term for a specific threat or in the longer term for more general security reasons, it should not be possible to book travel through the travel agent, although it is of course possible for someone to slip through the net if they buy their tickets independently. As the interviewee concedes, "No company can say, hand on heart, that it has a totally foolproof travel system." The security team runs security programmes to develop awareness among staff.

The team is required to review its security responsibilities and must sign a letter of assurance confirming compliance with the policies and standards, as set out in the governance processes. "As a corporate service, we are required to visit every country on a rolling basis. Low threat countries are visited approximately every five years, medium threat ones every 3 years, and high threat countries every 12-18 months or so." The interviewee explains that the decentralisation of responsibility for security means that the central team has a limited hands-on role with local managers, "We have what senior management calls a 'light touch' on security. We give responsibility to managers and they have local advice to make sure they are conducting security in accordance with the security standard. I would probably like to do a little bit more, but it seems to work for us." The effectiveness of the corporate security team is judged annually by the extent to which it meets the tasks and targets set on its annual business plan. The interviewee was not able to produce figures for the total number of people security incidents, although he did confirm that all incidents are required to be reported. This process is managed at the local level and local managers decide which ones to report upwards. They have no specific guidelines about the types of incidents they should be reporting, although it is mandatory for all fatalities to be reported and then investigated by a board member.

The company regularly benchmarks its security policies and procedures against those of peers. The interviewee explains, "The most recent major benchmarking exercise we carried out was in 2001. We also benchmark on a day-to-day basis. I am a member of a number of committees, and see this type of networking as incredibly important in being able to do my job. We benchmark mostly against companies in our own sector, but also many other different types of companies, but generally it is companies of a similar size. We also get benchmarked against by other companies on a regular basis." He notes that the board implicitly expects them to benchmark as it is within the overall requirements that all group services do this.

Links with governments

The interviewee expressed disappointment but some sympathy for the dilemma that the FCO's travel advice is aimed at a broad audience and so is not able to meet business-specific needs more directly. He would like to see the Government do more, "Their website tends to be aimed more at the lone backpacker who is travelling without back-up. There isn't much offered by the FCO in terms of corporate security. It's very patchy. I would like to see closer co-operation. I would like to see a new organisation. It doesn't have to be on the same scale as OSAC, but something along those lines would add a lot of value." He is realistic of the pressures facing the FCO, "I understand that governments have to be careful about the political signals they are sending out and that their advice has to be general rather than specific. We do get specifics off-the-record, though." He also admits that their size is an advantage for them, as it means they have lots of their own people on the ground gathering information and so are less dependent on government information than smaller companies. He also has regular contact with the Security Department at the FCO which is responsible for embassy security, along with the Economic Policy Department and some of the country desks. "It adds value to the work we do." The company also has contact with the governments of many other western countries.

The company also has contacts with British embassies, and is supportive of the approach they take, "They tend to have a pragmatic approach and that is very helpful." He also notes that embassy staff tend to have a very positive attitude, "Whenever we go we are able to see people in the embassy and they are always co-operative. I have never had a problem. This does, of course, vary depending on the size of the embassy, the size of our operations in the country and their resources for dealing with security."

5 Best practice

There are currently no commonly agreed standards of best practice offering companies guidance on how they should manage the security of their staff overseas. Advice about the most effective types of personnel security management systems, methods of ensuring information gets through to staff, and ways of organising travel systems would give companies a benchmark against which they, their staff and their stakeholders could measure them; and best practice could also clear up some of the ambiguities about legal responsibility raised in chapter two. While much of this is happening within membership organisations, because of the profile of members it tends to be limited to a small number of, usually, large multi-nationals or companies in particular sectors, which prevents the information from reaching the business community as a whole.

Best practice in relation to corporate personnel security would be guidance for companies about what they should be doing for their staff and would, in short, interpret what is meant by reasonable within the context of employees and their families living and working overseas on company business. It would flesh out the detail needed to answer the questions raised in chapter two, such as the balance of responsibility between companies and employees and the extent to which companies should be responsible for staff in their leisure time. It might set out procedures a company should observe, such as not allowing employees to travel to high risk countries without receiving detailed briefings, insisting that all families receive briefing packs before departure, and having a well-publicised security page on their intranet site that staff can access to find out what their company is doing for them.

This is one of the most important aspects of the work of the HSC and HSE, which develop and communicate standards of best practice for the effective management of health and safety in the workplace. Best practice can flesh out the law, which by its very nature tends to be fairly basic. It is also able to keep pace with developments without requiring large-scale revisions to the law. The law can then be left to set in stone those requirements that should not be open for negotiation. For instance, companies over a certain size might be required to have a dedicated corporate security manager. It would be less easy to set out preferred responses to specific threats or incidents, as these would be dependent on a number of quickly changing factors. The case studies highlight examples of what some companies are doing.

While there are no commonly accepted standards best practice is being developed informally. Many of those companies with a corporate security manager – usually the largest or most experienced overseas operators – already share experience and learn lessons through their membership of organisations such as the International Security Management Association (ISMA), the Risk and Security Management Forum (RSMF), The Security Institute, ASIS-International or the Guild of Security Professionals. One corporate security manager commented, “My board encourages me to network. I am a member of ISMA, which isn’t cheap, but we believe we have to benchmark externally rather than internally.” Some companies do this on a sectoral basis, too. The International Association of Oil and Gas Producers (OGP) works to spread best practice among its members, and it has the added value of being able to concentrate on issues specific to oil and gas companies. More informally still, corporate security managers of some large companies, including banks, meet regularly to compare notes, although this does not happen through any institutionalised network or organisation. And the corporate security managers of the large multinationals are assessing what they do on a day-to-day basis; finding out what peers in other companies are doing, how they are responding to the same threat, analysing the precautions they have in place, and so forth. One company representative commented, “A lot is shared informally and off-the-record, as happened recently in the build up to the war in Iraq. That type of contact is invaluable.”

In the absence of a comprehensive legal and policy framework to cover corporate personnel security overseas these disparate efforts are not being harnessed centrally. Most activity tends to be within those sectors where the risks are highest, either because of the nature of the work or the markets in which they operate, for example pharmaceutical companies, the extractive industry and tobacco and defence companies. It is also driven by security professionals, which means that lessons are generally only passed on through corporate security managers. Those companies without this function – usually the smaller or less experienced ones and the ones most in need of help – tend to miss out. One security expert commented, "As usual, the voice of the small- and medium-sized companies is not heard in security debates." There seems to be an expanding gulf between what might be termed the security 'haves' and the security 'have nots' in the business community. Guidance on what constitutes best practice would help those less experienced companies to get started and would enable the larger companies to continue to develop their policies. A centralised and co-ordinated best practice system would build on and maintain this momentum and help to ensure that the whole becomes more than the sum of its parts. As the next chapter shows, this is one of the features of the US Government's OSAC organisation, for which there is widespread support among companies.

Case study 6

The role and management of corporate security within the company

The interviewee reports to a board member and has regular contact with the CEO, the Chairman, the Chief Financial Officer, and the Director of Human Resources. This contact is informal rather than formal, on an individual basis rather than with the board as a group and is usually in response to an incident. He does, though, report to the board on Turnbull, and has a structured Turnbull process. He believes that security per se is a strategic risk for the company, but not personnel security in particular, "It is not a big risk in terms of its potential impact on the business." The interviewee presents to the audit committee, which is made up of non-executive directors. As well as giving an overview of corporate security, he is also required to produce statistics on losses from crime and fraud.

Legal responsibilities

The interviewee regards the company's legal responsibility to be to "look after the health and safety of employees and contractors and anyone else who comes into our premises. This extends to families overseas and security underpins it." He also expressed his own responsibility as extending to ensuring that his board is protected and is not liable should something happen. This is about having good measures in place and ensuring the company is doing all it can to protect employees. He believes that the company is meeting its legal requirements, "In my experience I would say we are meeting our legal requirements. We seem to be offering a very good service. If we weren't I would want to plug any gaps as soon as possible." The interviewee also believes that employees have to take on board a certain amount of responsibility, although he admitted that when they travel overseas the balance of responsibility between them and the company needs to shift, "Individuals need to take responsibility for safety as well as the company; it is a joint responsibility. However, when people go overseas they can find themselves in different and difficult situations so there is more of an onus on the company." The corporate security team is able to access legal advice from the company's in-house team of lawyers, although he did admit that he feels he may not have all the information he needs.

Personnel security policies and procedures

The company uses a variety of methods for communicating both advice and policy to employees. There is a corporate security and travel section of the company's intranet site, they issue email updates, and their in-country security teams liaise with travellers. The way they communicate depends on the issue being addressed. As the interviewee notes, "Our job is to turn on the customer and to cater for their needs. This is difficult in a large company; you need to be creative. I am constantly trying to break down barriers between security and the rest of the company." He believes corporate security departments need to strike a delicate balance in what they communicate and how, "You need to get a balance between too much and too little information. We don't want to scare people off working in a particular area when there is no need to."

The interviewee believes that the effectiveness of the corporate security team is measured by the board through relationships. "As long as they feel confident in your abilities; they don't want the finer details of security." He also benchmarks the department's work on an informal basis through membership of various security associations. He also uses the insurance risk review process as a form of measurement, "They mark us on a number of different controls and the more control you can show the lower your premiums are." He has not been through a formal benchmarking process, but plans to this year and will do this through various professional associations. His board actively encourages him to network. "I am a member of ISMA, which isn't cheap, but we believe we have to benchmark externally rather than internally."

Links with governments

The company has a link on its travel website to the FCO, but the interviewee has never had any contact with the FCO himself. He does, though, have access to information on the terrorist threat within the UK from contact with the Security Service due to the nature of the company's business. The security team deals with UK embassies as and when, but doesn’t have contact with local governments on the ground.

6 OSAC: The Overseas Security Advisory Council

OSAC was set up in 1984 to be a bridge between government and the US business community around issues relating to security overseas and is based on the principle of partnership between the two. OSAC's objectives are shown in the table below, and it is interesting to note that the link is made between effective security and business competitiveness.

Table 1: OSAC's Objectives

- **To establish continuing liaison and to provide for operational security co-operation between State Department security functions and the Private Sector.**
- **To provide for regular and timely interchange of information between the Private Sector and the State Department concerning developments in the overseas security environment.**
- **To recommend methods and provide material for co-ordinating security planning and implementation of security programs.**
- **To recommend methods to protect the competitiveness of American businesses operating worldwide.**

Services for members

OSAC offers a number of services to its members. They fill the gaps that have been identified in previous chapters, notably information about security risks and a common understanding of best practice in managing them. The organisation also indirectly raises the profile of corporate security within the US business community. The central administration of the organisation, which includes the research and management teams, and administrative and technical support, costs approximately $1.5

million dollars per year, which is equivalent to less than 2 per cent of the FCO's consular budget for 2002. This does not, however, include staff time in US embassies. All the costs are borne by the US government, although corporate members have to bear their own costs where they occur, such as the travel and accommodation of those business representatives carrying out work on behalf of OSAC or attending OSAC meetings. Its services are outlined in the following table:

Table 2: OSAC's Member Services

- Information and analysis. Its information is drawn from the private sector, the State Department and other government departments, intelligence agencies, law enforcement agencies, OSAC's in-house research team the Research and Information Support Center (RISC), US embassies, and the media.
- Off-the-record briefings by OSAC RISC staff.
- Web site. As well as information and briefings, the site has facilities for companies to report incidents, field questions for OSAC staff and corporate peers and give feedback.
- Email up-dates, which are sent to your desktop by 8.30am each day.
- Regional Security Officers (RSOs) in embassies. They are available for information and advice.
- Country councils. These are 'self-help' groups organised by representatives of the business community themselves.
- Benchmarking and best practice guides for companies on various aspects of effective security management.

Work through embassies

One of the most important features of the OSAC model is the fact that the US Government does not see its role as being limited to being a service-provider and information source. At the heart of the system is the assumption that the Government's role is not to do business's job for it, but to help companies to help themselves. A good example of this is the country council. A country council is a group of company representatives in a particular country or region. They are able to use the embassy as a base and the RSO[iii] is available to facilitate their contact with one another and with important locals, but the council is run by the business representatives themselves. As OSAC literature explains, "These organisations encourage managers of US enterprises with security responsibilities to organise themselves to cope with security problems by pooling their resources."

As of November 2002, there were 49 country councils, which was a 30 per cent increase on the year before. There are ambitious plans to significantly increase this number over the next couple of years. Companies claim to benefit enormously from this framework, not only from the up-to-date information they receive both from the embassy and from peers, but also from the networking opportunities with local officials, one of the needs identified by corporate security managers. The Country Council in Colombia is an excellent example of what can be achieved through engaged partnership:

The council has 81 companies as members, with 29 guest companies, and averages 73 attendees per meeting, illustrating the value of the initiative to the American business community in Bogotá. It has active links with the RSO in the US embassy, the American Wardens Network in the embassy, Colombian government authorities, the National Association of Industries (ANDI) and the local chapter of ASIS. Its regular meetings cover the full range of security threats for companies working in Colombia, such as kidnapping, extortion, terrorism, and insider threats. These sessions tend to cover case analysis, preventative measures, briefings from the authorities, recommended security measures, crisis and emergency planning, and tips on security audits.

[iii] The US government has a network of 450 Regional Security Officers (RSOs) in their embassies and consulates around the world. As well as non-business-related duties, such as embassy security, RSOs spend approximately one-third of their time acting as the point of contact on the ground between OSAC and the US business community.

The council also has a crisis management team, which meets in their emergency control centre when critical security events develop and reports on the conclusions and guideline recommendations for members. It has developed impressive channels for communicating with members during a crisis, including a phone and radio system that 42 companies have signed up to. As with all country councils, it is financed entirely by the companies themselves and is a useful forum for organised contact between the business community and the embassy.

Best practice

OSAC is also active in promoting best practice among the US business community. It publishes booklets on particular aspects of safety and security. These include *Security Guidelines for American Families Living Abroad, Security Guidelines for American Enterprises Abroad, Emergency Planning Guidelines for American Businesses Abroad, Security Guidelines for Children Living Abroad, Emergency Evacuation Guidelines for American Businesses Abroad,* and *Personal Security for the American Business Traveler Overseas*. There are also informal opportunities for benchmarking, which in many ways are a by-product of the system rather than an outright aim. This happens through meetings, either in the State Department or in embassies around the world.

Companies note the value of the informal side of OSAC membership. One corporate security manager explained, “The formal is taken as read. What really gives OSAC life is the informal element.” But this only happens effectively precisely because of the formality of the system, which encourages inclusion rather than exclusion and where there can be openness between civil servants and business people without any inference of impropriety.

Partnership through trust and results

This type of partnership is only possible where there is total trust. Research seminars and interviews have shown that OSAC members feel they get genuine value from their membership, that their needs are taken seriously by the US Government, and that there is an appreciation by the State Department of what companies bring to the table. One member commented, “I think that they operate an excellent system of information sharing and security briefings for all US companies operating abroad.” Another said of his company’s contact with OSAC, “The value of this relationship is significant.” The status of the organisation is underlined by the fact that the Secretary of State addresses its annual conference, and in 2002 placed adverts in a number of national business weekly magazines urging US companies to sign up. This level of support is crucial for the success of OSAC. One of those interviewed commented, “The US government is much happier to sit down with business and let their analysts talk about things.”

Case study 7

The role and management of corporate security within the company

The interviewee, the Group Security Manager, reports to the Group Financial Director, who sits on the company's main board and is the only executive director other than the Group Chief Executive with international responsibilities. He has regular contact with the board and is able to liaise with individual board members as and when he needs to. He is usually requested to give a briefing to his boss on current security issues ahead of the board meeting, usually in the form of a phone call, although his boss receives regular up-dates anyway. He also has a reporting line through his boss into the Group Audit Committee. He believes the board judges him according to the number of problems he doesn't take to them, and is judged by both short and long-term indicators, as with any other senior executive in the company. He believes that the board views personnel security as a strategic risk, as it is on the company's risk register. This is partly related to catastrophic incidents and succession planning, but also "not least because our processes are totally dependent on personnel." Contact with other departments is significant, particularly internal audit, compliance, legal, corporate communications, although less so with human resources. He sits on the group risk committee.

Legal responsibilities

The interviewee defined the company's legal responsibilities for staff within the context of its corporate social responsibility policy, "[through this] we have pretty much nailed our colours to the mast. We treat all staff pretty much the same in relation to security." He also believes there is an important responsibility for individual employees to play their part, too. "We can show we have made information and assistance available, but ultimately the final responsibility lies with staff. Individuals choose whether to check the advice, whether to follow it or whether to change their plans at the last minute and so slip through our nets."

The corporate security team's legal advice comes mainly from the company's group legal department and the group health and safety department. They also consult outside specialists, depending on the issue. He believes they have all the information they need or are able to have access to it. But as he acknowledges, "This is an area where it is easy to get caught out. I always try to find out through my networks whether there is anything I am missing." In terms of the company's commitment, he believes the company always tries to go beyond their basic obligations, "We are an organisation that would seek the moral high ground so we probably tend to go above and beyond our requirements."

Personnel security policies and procedures

The company consciously does not have a formal travel policy, other than to risk assess every journey. Because there are relatively few trips to higher risk countries or that would be deemed high-risk journeys, the security team is able to assess each journey individually. The interviewee gives a specific example, "We recently had a situation where four key players all needed to be in the USA for a meeting. It would have been crazy to have them all on the same plane, but we assessed their roles and it was decided that they could go on two rather than four separate flights because of the roles they have. The main priority was to ensure that we managed the risk versus the business requirement appropriately."

Because the company has relatively few travellers, the interviewee believes that communication is less of a problem for them that it might be for other companies. "It is usually a small number of senior people and we are able to communicate with them on a one-to-one level." They assess trips on a case-by-case basis, "While the FCO was warning against travel to India and Pakistan I had one man who wanted to travel to India on a business essential trip. He was a very experienced traveller who knew the country well. We spent one and a half days assessing the risk on that journey and eventually agreed he should go, but with a number of safety nets in place." He has seen a rise in interest since September 11th and believes this has had a positive impact, "9/11 made people who thought security was irrelevant more aware that security issues are real. We carried out a publicity campaign within the company to raise awareness and I would say that people are now safer, in large part because they are more aware. For example, each year some businesses run senior management conferences in various parts of the world. Prior to 9/11 I was not normally asked to carry out a risk assessment, but now I invariably am." There is now significant demand for the services of corporate security, and they have had to increase the number of crisis management courses they run.

Minor personnel security incidents that take place overseas are not reported to the group, but there is awareness that they are a frequent occurrence. "Minor incidents happen more of less all the time. Significant security incidents are rare, though; we have perhaps one or two each year on average, but none so far have been fatal. While I have been at the company there have been just two significant incidents involving staff." They have had near misses, though, "We had people in Bali, for example."

The interviewee believes that his effectiveness should be judged in the same way as any other senior executive, "Does anything I do affect the value of the company, positively or negatively?" There are a number of mechanisms in place aimed at monitoring effectiveness, such as a review as part of the audit process, there are regular forums for feedback, and the security team goes out to businesses on the ground for feedback, too. Company CEOs are also required to sign off to say they are compliant with the company's corporate governance manual, which contains a number of security policies.

The interviewee places a lot of importance on benchmarking, which happens on an almost daily basis among peers. He is a member of ISMA and is involved in benchmarking with other members. "I often call and get called for views when we are working in similar areas. This is useful because some people have more experience in certain areas than others and you might also want to spread a good idea you've had to others." He believes it has benefits beyond the day-to-day running of the security department, "It is reassuring to boards and stakeholders that you have benchmarked against other companies. For example, in the lead up to the war in Iraq there was significant debate about travel, and in the security community we were benchmarking like mad. I was able to back up my views with those of respected peers."

Links with governments

The interviewee is registered with the FCO website to receive all their updates and makes himself aware of the FCO's advice. However, he does not believe it is particularly useful, "It only very occasionally adds value to my work. It is useful to be able to quote it and say if and why I agree or disagree with it." But he does believe there is potential for the Government to play a valuable role in helping companies to keep staff safe. He sees that the FCO and embassies are staffed by very able individuals and like other interviewees he believes the UK has some of the most effective and sensible methods of analysis in the world that would be helpful to tap into. The failing, though, is the overall approach of the British Government to business, "What is required is a more business-oriented, truly international attitude in support for UK plc and some way of reducing the fear of commitment on the part of civil servants. In Britain, unlike the USA or our European neighbours there is a culture of secrecy. The view seems to be that business is a dirty word. There is an elitism, which may be disappearing, that gives the impression that they don't want to deal with commerce. The flip side of that is that in other departments, the calibre of staff involved is not nearly as high." He does, though, understand the constraints under which they have to work.

In contrast, he has a positive view of the approach of the US Government, "It is much easier to get information from the State Department than the FCO. There is a much more open relationship. It's far from perfect, but at least it is there. The value from this relationship is significant. Of course, the Americans tend to work in a different way to the Brits; they are more reactive, but it is helpful to know what they are thinking and it is useful to know you can call the RSO, that he can identify you and have some comfort in being able to talk to you." He also suggests that if there were partnership between the UK Government and the business community many companies would be able to input, too, "It need not be a one way street. Companies have a lot of information that would help in understanding emerging trends on the ground. Being able to pool this type of information would be of value to all. I would be willing to share this type of information if there were a partnership." He also has contact with local governments on the ground.

7 Case study conclusions

As part of the research for this project, seven companies were selected to act as case studies. The member of staff with overall day-to-day responsibility at a corporate level for security – including personnel security – was interviewed, and companies also supplied supporting information in the form of policy documents, documents given to staff, training videos, and access to their intranet sites. There was a large degree of co-operation and help from the companies.

The aims of the case studies

It is hoped that these case studies will provide a more in-depth understanding of the way personnel security is managed within companies. They are not put forward as a representative study – they are some of the largest multi-nationals and they are all companies committed to the value of corporate personnel security, as exemplified by their willingness to take part in such a study. It has not been possible given the scope of the project to verify the answers that were provided, and the material should be read with this in mind. It is also hoped that on a practical level this information will be useful to corporate security managers and their companies in comparing what they do with some of their peers.

The topics covered reflect the research aims of this project. They focus on personnel security, with some broader questions, too. They include:

- Understanding of the legal framework as it affects corporate personnel security
- The use of best practice: the extent to which companies know what their peers are doing; whether standards of best practice are being developed informally; and if so, how they work
- The status and role of corporate personnel security within the company

- The companies' relationships with the UK Government, other western governments and governments in the emerging markets in which they operate
- The judgments of those interviewed on the changing perceptions of risk among staff within their companies

About the companies

They come from a range of different sectors: pharmaceutical, banking and finance, defence, extractive, tobacco, and communications. All of the companies are large multi-nationals listed on the London Stock Exchange. Most are considered by their peers to be some of the most effective at managing corporate security, with a number being some of the most frequently benchmarked against companies in the world. They are likely, therefore, to represent the best prepared companies in terms of corporate security.

It is worth noting that the individuals interviewed are themselves some of the most experienced and most respected corporate security managers in the country. The interviews also, therefore, provided a useful opportunity to solicit their personal opinions on a range of related topics. Their comments are shown both in the case studies themselves, as well as being scattered throughout the report itself.

The overall conclusions

A number of conclusions can be drawn from these case studies:

Understanding of the problem and the response

- Even some of the largest companies are at a very early stage of development in relation to corporate security. One interviewee commented, "If you ask me these questions again in a year's time you might get a different response. I have started out with a blank sheet and it's still very early days in development."

- Companies have a poor understanding of the extent of the problem as it faces them. One person commented, “I have no idea how many people security incidents we have. I could work out the major incidents, but not the smaller ones.” None were able to produce figures.
- There do not appear to be systems in place to measure the effectiveness of corporate personnel security policies and procedures. That is not to make any judgment about whether or not those in place are successful; in fact, that is beyond the parameters of this research project.
- The companies interviewed are benchmarking a lot. This happens on both formal and informal levels and covers everything from system and management questions to queries about day-to-day decisions, such as when and how to evacuate in the build up to the Iraq war. All interviewees were keen to stress that corporate personnel security is a non-competitive area of the company’s business, and this enables them to share information and advice with peers in other companies. The benchmarking seems to be limited to a small number of companies, though, and all are very large multi-nationals.

Support within the company

- Most interviewees felt they had reasonable support from their boards, but there were varying degrees of engagement.
- All agreed that their board had been more interested in security since September 11th. There seems to be a heightened awareness of the risks.
- All said they have good links with other departments right across the company, from human resources and legal to public affairs and compliance.

Legal responsibilities

- None of those interviewed saw the legal framework as being problematic and felt confident about what their legal responsibilities are to staff. However, it was interesting to note that interviewees varied in what they thought these responsibilities were, indicating either that the law is not clear or that there are ambiguities on their part.

- All agreed that individuals have an important responsibility for their own safety. Many related this to the corporate culture. For example, one said, "The ethos here is that it is up to everyone to look after security but that they need help to support them, but not to nanny them. Some companies go to great lengths to tell people what to do and what not to do. It's not like that here. We tend to be the first in and the last out. There is an understanding that we have to look after our staff but there needs to be a reliance on people to get the job done. We expect individuals to be proactive in looking after themselves. All of these things are unsaid."

- Companies are using a range of methods to communicate the risks to their staff, from the company intranet site and newsletters to awareness campaigns run in individual buildings or sites. There was no clear view among most companies, though, about the extent to which the messages were reaching staff.

- Corporate security communication tends to be directed at those with responsibility for security, rather than individual members of staff.

The company

- The company's structure can be an important limiting or enabling factor in its ability to be effective in tackling security threats to staff. In particular, a number of interviewees working within decentralised group structures complained that this made their jobs a lot more difficult.

- The effectiveness of security practices at the local level can be personality-led. One interviewee noted, it “depends on the energy and enthusiasm of the local site manager.”
- A one-size-fits-all approach to security is not likely to be successful because of the number of variables at play. Factors such as the size of the company, the number of staff they have working in emerging markets, the level of the threat, and the experience of the travellers concerned should influence the way the company manages corporate personnel security in emerging markets.

Links with governments

- Almost all of those interviewed were unhappy with the information, advice and other services offered by the FCO in London and its posts around the world. There was considerable demand for a stepped-up service.
- There was a general feeling that the FCO has very good people, who try to be as helpful as is possible but that the value-added by this contact is minimal because there is no proper system within which it can take place, and as a consequence there are few resources available and the service they do receive is personality-driven. One interviewee commented, “We tend to find that their resources are limited and the standard of care is people-dependent rather than organisational-dependent.”
- Many report that they receive more detailed briefings from FCO personnel, but this is done off-the-record and is through personal contacts. One interviewee noted on the differences between the US and UK approaches, “I have had help in the States in a way that wouldn’t have been possible in the UK

without having been in the public service."

- There was widespread support for the work of the US Government. On the whole, the strengths of the US approach lay in having a structured system, the openness of the US Government, and the strong commitment to the value for both companies and the Government of a strong partnership between the two.
- The business community does not seem concerned about receiving conflicting information and advice from different national governments. One commented, "Divergent information is a good thing. Commonality can suggest that not enough thought has been put into it. I prefer the challenge of different views."

SECTION FOUR: A NEW APPROACH TO CORPORATE SECURITY

This report argues that there needs to be a new approach in the UK to the management of corporate security overseas. Policy is currently hampered by a legal vacuum, a lack of understanding about the scale of the problem, a level of informality that limits effectiveness and barriers between the Government and the business community that send both into the ring with one hand tied behind their backs.

This report has shown that there are three important gaps in the legal and policy framework relating to corporate personnel security overseas:

– There is **no comprehensive legal framework governing corporate personnel security overseas in the same way that there is relating to health and safety in the workplace**. This means that those companies that want to do nothing are able to do so without recourse and those that want to do the right thing are left unclear about whether or not they are as effective as they could be. Employees are unclear about what they can reasonably expect their employers to do and the extent to which they should be looking after themselves.

– There is **a lack of publicly available information to aid the management of corporate personnel security overseas**. Firstly, companies claim they don't get enough information from the Government about the threat itself and there are no mechanisms for companies to contribute data that would be of value to the wider policy community. The absence of this information also makes it difficult for staff to make judgments for themselves about the risks they take when working overseas. Secondly, there are no commonly agreed standards of good or best practice for companies, apart from that being collated within a small number of membership and sector-specific organisations, which doesn't tend to filter down beyond the largest multi-nationals.

– There is **no mechanism for co-ordinating the work of the**

> **Government and companies to ensure that their collective effort is worth more than the sum of its parts**. Given the current security state around the world today, there has never been a better time to strike up a formal partnership to galvanise momentum and energy around this important challenge that governments and companies have in common.

In order to keep safe those working overseas for British companies, there needs to be:

1. Legal Reform

There should be clarity about the balance of responsibility between companies and staff in managing corporate personnel security overseas so it is clear what companies are expected to do, and the extent to which employees must take care of themselves. This could be achieved by **extending the scope of the Health and Safety at Work Act** to explicitly cover personnel security overseas. This would also allow foreigners working for British companies to take action when their employers fail to meet their security obligations. This would set a **British security standard**, with the Government using its influence to encourage other countries to follow suit. There should also be commonly agreed **standards of good practice** to offer guidelines to companies about how they should interpret the new law.

The research has shown that companies are managing personnel security through a range of different management systems. Within the parameters of this project it has not been possible to test whether some are more effective than others, but this element of **corporate governance** should be a subject for further study. Companies may, for example, be required to have a senior member of staff responsible for corporate personnel security. They may also require them to report directly to the main board to ensure that this is an issue that has salience at the top of the company and that security has been properly integrated into the business. This might also be underlined by companies being required to report on their activities in their annual reports.

2. Better Information

There is currently a **lack of information about the nature of the threat to staff** working overseas. While there is a plethora of analysis from a number of different sources – including the Government and private security companies – on the underlying causes of instability, such as political tension, social inequality, and so forth, there is little information about the impact this has on people on the ground. There are three ways that this situation could be improved. Firstly, **companies should record information** about actual cases as well as attempted cases. As the case studies showed, even some of the largest and best-prepared companies were unable to provide information beyond the most serious cases, although they admitted that minor incidents happen on an almost daily basis. This is essential in order to build up a full picture of what the risks really are for companies and their workforces. While certain gaps would probably persist, a centralised system would provide much better understanding. Secondly, **Government needs to provide more business-specific information** on the threat. This is discussed in more detail below. Thirdly, there needs to be a **central collation point for this information**, to bring together the data from companies, the UK Government and local governments on the ground. Only then will we have a rounded picture of the way in which security problems threaten workers overseas.

There is also a need for **more information on the best ways to manage the threats**. While much work is taking place to develop standards of best practice, with companies benchmarking against one another on the nature of their security management systems as a whole as well as day-to-day decisions, this information is not disseminated beyond a small number of companies. It is particularly concentrated within very large multinationals, and companies within certain sectors, notably the extractive industry, tobacco companies, and pharmaceuticals. Private security companies are also carrying out useful work, but this can be beyond the reach of smaller companies due to the cost. There needs to be a **focus on small- and medium-sized companies**.

3. A New Partnership Approach to Corporate Security

At the heart of this new approach must be the **breakdown of barriers between the Government and the business community**. As the research has shown, there are few contacts between companies and embassies on the ground in relation to security, companies feel the information they receive from the Government is insufficient and there is sense from the companies interviewed – rightly or wrongly – that the Government does not want to work with them. The founding principle of this partnership must be **value for all** – both have much to give and both will manage their security much more effectively if they work together than if they struggle along on their own.

The partnership must have a **formal status**. As the research has shown, much of what is being done at the moment on both the Government and the business side happens informally, either through networks or personal contacts. In a world that the Prime Minister has described as being characterised by insecurity[34] not only is this unprofessional, it is an inefficient way of delivering information to protect an important component of our national interest. A formal partnership would also give **visibility and legitimacy to the initiative**, which might encourage more companies to get involved.

The **UK Government should launch a Government-business partnership on security**. The US State Department's Overseas Security Advisory Council sets a precedent and illustrates how such a partnership could be managed and what it might hope to achieve. It should concentrate on the main gaps identified in this report: **information on the threat** and the **development of best practice guidelines**. It should work on two levels; firstly through the **FCO in London** and secondly through **embassies and high commissions on the ground**.

It is vital there are **sufficient resources available to deliver what should be ambitious goals**. The costs of administering the core team in London are likely to be modest; OSAC's headquarters in

Washington costs approximately $1.5 million per year. Supporting the partnership on the ground through embassies and high commissions would represent a significant investment over and above what is currently delivered. It is therefore important that the **business community contributes towards these costs**, either through an **annual subscription** or through **pay-as-you-use services**, while maintaining a core of publicly available information that meets the minimum requirements of the business community. **Cost should not prevent small- and medium-sized companies from entering into the partnership**, though. Research has shown that they are the highest need group and they should therefore be the principal target audience for the initiative. The business model must therefore find ways of subsidising their use of the services. These funds should also be used to ensure the partnership is **properly publicised throughout the business community**.

It will be important for there to be an **organisation responsible for administering this partnership** to ensure momentum is maintained, targets are set, and progress is continually monitored. This may need to be a separate organisation or it could form part of an existing government or business body. Regardless of where it lives, in order to be credible as a genuine two-way partnership and to ensure it is representative of the needs of both, it is vital that there are **business and government representatives on the management** board for the partnership.

This partnership has the potential to deliver far beyond the scope of this research on corporate personnel security in emerging markets. OSAC covers the full range of security threats to American companies and it would make sense to use the British partnership for **as wide a range of security issues as possible**. OSAC has also begun to play a valuable role in the US fight against terrorism at home. *The Unlikely Counter-Terrorists* argued that the business community needs to be much more involved in counter-terrorism at home, and this argument is gaining ground within domestic policy, security and intelligence circles. A

British partnership for security overseas could also have a **role in the UK** and in doing so, help to **break down the barrier between home and abroad in the search for security** and pave the way for more work in the domestic arena. Finally, it is important to **break down international barriers across borders**, and to look for ways of achieving greater co-operation between allies. A British partnership should look for ways to **forge partnerships with the US, European neighbours and beyond**.

Given the nature of the security environment around the world, now is the time to break down as many boundaries as possible – be they between public and private, home and abroad or with our allies. The rise of the security threat poses challenges. But it also brings great opportunities to use the energy and commitment around these issues to push for change in an area of policy traditionally characterised by secrecy, informal relationships and misunderstanding. The partnership suggested is about much more than creating a set of processes or a new bureaucracy. At the heart of its existence must be the aim of breaking down the assumptions that currently shape the way we frame and respond to security threats. It is hoped that this will bring the clarity and understanding that will make British interests safer overseas.

Notes

[1] www.investorwords.com

[2] *Travel Trends: A report on the 2001 International Passenger Survey*, National Statistics Office, 2002

[3] Originally, it was forecasted that growth between 2000 and 2005 would be 16.7 per cent, taking into account the economic downturn. This was then re-forecasted to take into account the impact of September 11th 2001. Down but Not Out, press release from ABTA 02 November 2001 (http://shaftesbury.venus.co.uk/abta/news/2001/11/1135.htm)

[4] The Stationery Office, *Travel Trends: A report on the International Passenger Survey*, 2002

[5] Quoted in Mabel Msonthi, 'Stretching their Wings', *Guardian*, 11th March 2002

[6] http://www.mori.com/digest/2002/pd020322.shtml

[7] Quoted in Mabel Msonthi, 'Stretching their Wings', *Guardian*, 11th March 2002

[8] Cendent Mobility, 2002 Benchmark Study, *New Approaches to Global Mobility: New challenges and issues relating to cross-border transfer activity*, 2002

[9] Chris Brewster, 'They Shall Not be Moved: A global view of the HR profession', *People Management*, 21, February 2002

[10] Faisal Islam, 'How these people are doing more for the Third World than Western governments', *The Observer*, 20th April 2003

[11] National Statistics Office: www.statistics.gov.uk/statbase/expodata/spreadsheets/D3804.xls

[12] *Economist*, 'Business in Difficult Places', 25th May 2000

[13] Rachel Briggs (ed), *The Unlikely Counter-Terrorists*, The Foreign Policy Centre (2002)

[14] Survey carried out by Janusian Security Risk Management, the results of which were presented at a conference on 1st April 2003.

[15] Quoted in Securing the Knowledge Enterprise, Globally, Armor Group, 2001

[16] Quoted in Mabel Msonthi, 'Stretching their Wings', *Guardian*, 11th March 2002

[17] www.thebci.org

[18] Cendent Mobility, 2002 Benchmark Study, *New Approaches to Global Mobility: New challenges and issues relating to cross-border transfer activity*, 2002

[19] Health and Safety at Work etc Act 1974 SI 1974/1439, The Stationery Office, 1974, ISBN 0 11 141439 X

[20] www.hse.gov.uk

[21] For more details about the case brought against Cape plc see Halina Ward, *Corporate accountability in search of a treaty? Some insights from foreign direct liability*, Briefing Paper 4, RIIA, May 2002. This paper raises some useful points about the challenge of holding companies to account across national borders, referring to the case against Cape

plc and Thor Chemicals, both in South Africa.

[22] The author does not take a view on this case, but raises it as proof of concern about the lack of clarity about corporate duty of care. There has been considerable coverage of this case, which also involved Grainger Telecom. A useful reference is a 'File on Four' programme on the case on Radio Four in October 2000.

[23] Wicker and August, "Working Lives in Context: Engaging the views of participant analysts", reproduced in *Person Environment Psychology: New directions and perspectives*, Walsh et al (eds.), 2000

[24] Quoted in Rachel Briggs, *Travel Advice: Getting information to those who need it,* The Foreign Policy Centre, 2002, page 12.

[25] Jane Nelson, *The Business of Peace: The private sector as a partner in conflict prevention and resolution*, The Prince of Wales Business Leaders' Forum, 2000

[26] For more information on the types of issues that companies need to consider when communicating travel advice to their employees, refer to Rachel Briggs, *Travel Advice: Getting information to those who need it*, The Foreign Policy Centre, 2001

[27] Quoted in a seminar on travel advice, held at The Foreign Policy Centre on 4th July 2002.

[28] Paul Barker, Managing Risks to Employees on Overseas Assignments, unpublished MSc dissertation for the Study of Security Management, Scarman Centre for The Study of Public Order, University of Leicester

[29] For more details, see the event report from the seminar: 'Corporate Security and Reputation: Making the business case for corporate security', available at www.fpc.org.uk

[30] Simon Webley and Elise More, *Does Business Ethics Pay? Ethics and financial performance*, Institute of Business Ethics, 2003

[31] Securing the Knowledge Enterprise, Globally, Armor Group, 2001

[32] Rory Knight and Deborah Pretty, *Reputation and Value: The case of corporate catastrophies*, Oxford Metrica, 2001

[33] Ian Springsteel, 'Dangerous Liaison', *CFO Magazine*, August 1998

[34] The Prime Minister's 2003 New Year message can be read at http://www.number-10.gov.uk/output/Page6904.asp

Also available from The Foreign Policy Centre

Individual publications should be ordered from
Central Books, 99 Wallis Road, London, E9 5LN
tel: 020 8986 5488, fax: 020 8533 5821
email: mo@centralbooks.com

To read online go to www.fpc.org.uk/reports

(Subscriptions are available from the Centre itself)

THE KIDNAPPING BUSINESS

By Rachel Briggs
March 2001; £14.95; ISBN 1-903558-16
Kindly supported by Hiscox, Control Risks Group, ASM Ltd., Marsh Ltd and SCR

THE UNLIKELY COUNTER-TERRORISTS

Rachel Briggs (editor) with essays from John Bray, Bruno Brunskill,
Roger Davies, Bruce George MP, Dr Sally Leivesley, Richard Sambrook,
John Smith, David Veness and Natalie Whatford.
November 2002; £19.95 ISBN 1-903558-21-2
Kindly supported by BAe Systems, Control Risks Group, and RSMF

TRAVEL ADVICE:
Getting information to those who need it

By Rachel Briggs
August 2002; £19.95 ISBN 1-903558-16-6
Kindly supported by Thomas Cook Tour Operations

KEEPING YOUR PEOPLE SAFE:
The legal and policy framework for duty of care

Corporate Personnel Security in Emerging Markets Working Paper 1

By Rachel Briggs
2003; £4.95 ISBN 1-903558-24-7
Kindly supported by Armor Group, Control Risks Group, Group 4 Falck, GSK, HSBC and Shell

THE ROLE OF THE UK GOVERNMENT

Corporate Personnel Security in Emerging Markets Working Paper 2

By Rachel Briggs
2003; £4.95 ISBN 1-903558-20-4
Kindly supported by Armor Group, Control Risks Group, Group 4 Falck, GSK, HSBC and Shell

IRAQ AND WORLD ORDER

By John Lloyd
February 2003; £4.95 ISBN 1-903558-27-1

'Powerfully outlines the case for systematic intervention in totalitarian-terrorist and failed states,'
Donald Macintyre, The Independent

AXIS OF ANARCHY:
Britain, America and the New World Order after Iraq

By Andrew Tyrie MP
In association with the Bow Group
March 2003; £4.95 ISBN 1-903558-26-3

'Especially interesting at this moment of uncertainty about the future of the Middle East and of the international community as a whole,'
Chris Patten, EU External Relations Commissioner

RE-ORDERING THE WORLD:
The Long-Term Implications of 11 September

Mark Leonard (editor), with essays by Ehud Barak, Ulrich Beck,
Tony Blair, Fernando Henrique Cardoso, Malcolm Chalmers, Robert Cooper,
Fred Halliday, David Held, Mary Kaldor, Kanan Makiya, Joseph Nye,
Amartya Sen, Jack Straw and Fareed Zakaria.
March 2002; £9.95 Available online at www.fpc.org.uk/reports
'Caused a storm …' ***The Observer***

THE POSTMODERN STATE AND THE WORLD ORDER

By Robert Cooper
In association with Demos
June 2000; £8.95, plus £1 p+p ISBN 1-814180-010-4

'Mr Cooper's pamphlet explains, lucidly and elegantly, how the emergence of what he calls the postmodern state has changed international relations,' ***New Statesman***

PUBLIC DIPLOMACY AND THE MIDDLE EAST

By Mark Leonard and Conrad Smewing
In association with The British Council
February 2003; £19.95 ISBN 1-903558-25-5

'Highly interesting,'
Neil Kinnock, Vice-President of the European Commission

'This pamphlet will prove valuable in the work we are doing in the region,' ***Jack Straw, Foreign Secretary***

THIRD GENERATION CORPORATE CITIZENSHIP: Public Policy and Business in Society

By Simon Zadek
In association with DIAGEO and Friends Ivory & Sime
December 2001; £19.95 ISBN 1-903558-08-5

*'Zadek strikes at the very heart of this debate', **Craig Cohon,*** **Globalegacy**

NGO RIGHTS AND RESPONSIBILITIES: A new deal for global governance

By Michael Edwards
In association with the NCVO
July 2000; £9.95; ISBN 0-9053558-00-X

'Compelling and succinct',
Peter Hain

'A smart and insightful account of the changing role of NGOs…
a series of excellent policy recommendations',
David Held, LSE

Subscribe to The Foreign Policy Centre

The Foreign Policy Centre offers a number of ways for people to get involved. Our subscription scheme keeps you up-to-date with our work, with at least six free publications each year and our quarterly newsletter, Global Thinking. Subscribers also receive major discounts on events and further publications.

Type of Subscription	Price
□ Individuals	£50
□ Companies and Organisations (will receive ALL publications)	£200
□ Diplomatic Forum (Special high-level embassy scheme)	£500

Please make cheques payable to **The Foreign Policy Centre**, indicating clearly your postal and email address and the appropriate package, and send to Subscriptions, The Foreign Policy Centre, Mezzanine Floor, Elizabeth House, 39 York Road, London SE1 7NQ. For further details, contact info@fpc.org.uk