LLOYD'S

360

# UNDER ATTACK? GLOBAL BUSINESS AND THE THREAT OF POLITICAL VIOLENCE

# FACT:
# AROUND 20% OF INTERNATIONAL TERRORIST ATTACKS ARE DIRECTED AGAINST BUSINESS

The Memorial Institute for the Prevention of Terrorism (MIPT)

# UNDER ATTACK?

## GLOBAL BUSINESS AND THE THREAT OF POLITICAL VIOLENCE

# FOREWORD
## FROM THE CHAIRMAN OF LLOYD'S

**Geopolitical risk in its various forms affects most of us, but its impact on business is not often recognised or well understood.**

One estimate suggests the costs of political risk to the global economy could be $1 trillion, equivalent to a 0.25 percent "geo-political tax" on global GDP growth. Economies certainly benefit from stability and predictability and this research shows that business leaders are very concerned about the affect of regime changes or contract frustration, while they admit that they often understand little about the conflicts and politics they might encounter directly or indirectly as they seek to globalise.

21st century terrorism is a specific issue where the price of getting it wrong can be very high, and the solutions are rarely simple. In the aftermath of 9/11, close to 200,000 jobs were destroyed or at least temporarily relocated out of New York City. In the last decade, in addition to those who perished after 9/11, nearly 2,000 people have died in terrorist attacks on business alone, and around 20% of terrorist attacks are aimed at the business community.

This new research shows that business leaders believe they are operating in an increasingly dangerous world, and focuses on the risks which they specifically face from terrorism and political violence. It reveals that boards are spending an increasing amount of time discussing the associated risks. It also leaves little doubt that political violence has a significant and wide impact on both strategy and operations – from employee vetting to whether to invest in a given location. But the decisions taken are not always the right ones. There appears to be a significant gap between a growing risk awareness and tangible action actually taken by many companies, driven by a lack of understanding of the dynamics they encounter as they globalise.

This is coupled with a lack of awareness about the impact the organisation has on the environment in which it operates. Typically, business sees itself neither as part of the problem nor part of the solution in regions of conflict and instability. Accepting that business is at risk also means accepting it has a role to play. More active engagement can deliver real benefits to organisations – which go beyond strong risk management alone and can impact the company more widely than might be apparent at first.

For those of us operating in an increasingly complex risk environment, political violence may not always be top of mind. But in an era of increased globalisation, understanding and preparing for political violence has arguably never been more important for business. More than one of the organisations interviewed for this study has seen colleagues killed in politically motivated attacks. As recent world events have shown, political violence is not restricted to known 'hot spots', and the importance of reflecting changing political violence risk in corporate risk management strategy has never been greater.

**Lord Levene**
**Chairman of Lloyd's**
**April 2007**

# EXECUTIVE SUMMARY

## 1 BUSINESS LEADERS BELIEVE THAT POLITICAL VIOLENCE RISK IS REAL AND RISING

7% of companies have suffered collateral damage from acts of political violence, 5% have suffered a direct attack on their home country facilities and most believe that the risks are growing. More than one-half believe that business is now as much a target for attack as government, and think political violence will increase worldwide over the next five years, with terrorism and conflict set to become bigger problems than ordinary crime.

## 2 CONCERNS ABOUT POLITICAL VIOLENCE ARE PREVENTING COMPANIES FROM INVESTING WHERE THEY WOULD LIKE

Conflict and instability are significant barriers to foreign direct investment. Political violence has caused 37% of companies to avoid investments in overseas markets: one in five firms have foregone otherwise promising business opportunities for the same reason and nearly one-half of North American companies now think twice about locating key offices in large cities.

## 3 AS POLITICAL VIOLENCE RISKS EVOLVE, FOUR KEY THREATS ARE EMERGING

Companies must develop flexible risk management strategies given an increasingly interconnected economy coupled with a more complex risk environment. The protagonists in political violence are today increasingly amorphous militias and gangs. In addition, new forms of jihadi terrorism have different objectives to previous protagonists, including high casualty counts.

- **Supply chain risk is an increasingly important consideration – not least given energy security concerns.** Around 30% of respondents believe that their companies are exposed to collateral damage from an indirect attack, or to the impact of violence on supply lines and energy supply. North American and larger companies show even greater concern.
- **Many executives fear that IT systems could become a target for cyber-terrorism.** Terrorist technological capability is well known and, in response, over 40% of companies are increasing spending on IT security. Although there is little firm evidence that computer systems are becoming a major target, the possibility of attack creates a reason for companies to strengthen their IT security.
- **A new generation of home-grown terrorism is forcing businesses to tighten up procedures in areas such as employee vetting, the choice of sub-contractors and location of operations.** Investment in IT security, continuity plans and insurance spending are all rising as a direct result of these concerns.
- **CBNR (chemical, biological, nuclear and radioactive) risk is now perceived as a significant threat by almost one-quarter of companies.** A similar proportion is leading best practice in this area by developing and testing continuity plans to cover this risk.

# 4 PERCEPTION DOES NOT ALWAYS MATCH REALITY: BUSINESS NEEDS BETTER INFORMATION TO UNDERSTAND WHERE THE REAL RISKS LIE

Only 37% of business leaders believe that their companies have a strong understanding of the political violence risks they face. In addition, perceptions of risk appear to be driven by media headlines rather than rigorous analysis. One in ten companies do not systematically gather information on conflict risks at all. Of those that do, most rely mainly on international news coverage. Just 20% make use of the information available from specialised consultants, academics or non-governmental organisations (NGOs) that could help them to improve their analysis. Worse still, only 39% have a mechanism for employees to feed in data to help corporate analysis of political risk. Smaller companies do even less.

# 5 PREPARATION IS KEY BUT MOST COMPANIES NEED TO DO MORE AT THIS IMPORTANT FIRST STAGE

One-fifth of firms do not address the risk of political violence systematically. Almost one-quarter of all companies have no continuity plan at all and a further 14% believe that their plan is insufficient in the light of political violence. These figures are even greater for smaller companies.

# 6 COMPANIES THAT ENGAGE IN LOCAL CONFLICT ISSUES CAN BRING WIDE BENEFIT TO THE BUSINESS

Most businesses tend to try to be invisible in times of violence. Only a small minority say they would actively help to reduce levels of conflict and few see the link between their corporate social responsibility programmes (CSR) and the wider political risk environment. They may be wrong to adopt this attitude. Best practice is still evolving in this field, but a growing number of policymakers, NGOs and companies believe that business should play a more active role. This does not mean trying to solve political problems so much as driving economic development in ways that can help to deliver a more stable operating environment, with reduced operational risk and improved community relations.

# METHODOLOGY

***Under attack? Global business and the threat of political violence*** **was written in co-operation with the Economist Intelligence Unit, based on an extensive programme of research activity.**

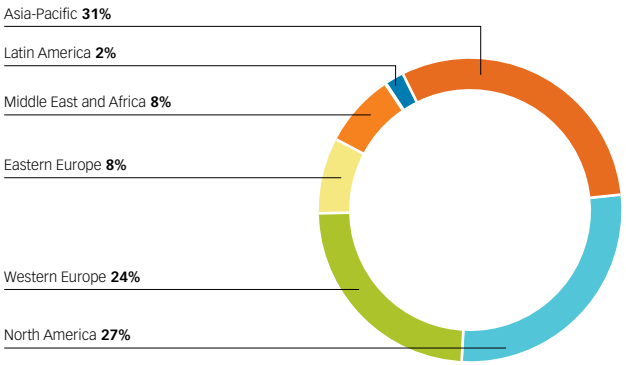
The Economist Intelligence Unit first conducted a global survey of 154 board-level executives to explore corporate perspectives on political violence. Of these executives, 58% are CEOs, presidents or managing directors.

The survey drew respondents from a broad spectrum of industries, with particularly strong representation from financial services, professional services, IT and technology, and manufacturing companies. A cross-section of large and small organisations was included to provide a broad business perspective on the issue.

To supplement the survey results, the Economist Intelligence Unit then carried out a number of in-depth interviews with senior executives, security and terrorism experts, NGOs and policymakers.

The Economist Intelligence Unit would like to thank the survey respondents and interviewees for their valuable time and insights.

**In which region are you personally based?**




**Which of the following best describes your title?**

| | |
|---|---|
| **Board member** | 12% |
| **CEO/President/Managing director** | 58% |
| **CFO/Treasurer/Comptroller** | 8% |
| **CIO/Technology director** | 5% |
| **Chief risk officer (CRO)** | 5% |
| **Other** | 12% |
| **Total** | 100% |

**What is your primary industry?**

| | |
|---|---|
| **Aerospace/Defence** | 0% |
| **Agriculture and agribusiness** | 3% |
| **Automotive** | 1% |
| **Chemicals** | 1% |
| **Construction and real estate** | 4% |
| **Consumer goods** | 5% |
| **Education** | 1% |
| **Energy and natural resources** | 7% |
| **Entertainment, media and publishing** | 3% |
| **Financial services** | 26% |
| **Government/Public sector** | 0% |
| **Healthcare, pharmaceuticals and biotechnology** | 6% |
| **IT and technology** | 12% |
| **Logistics and distribution** | 0% |
| **Manufacturing** | 8% |
| **Professional services** | 15% |
| **Retailing** | 2% |
| **Telecommunications** | 2% |
| **Transportation, travel and tourism** | 4% |
| **Total** | 100% |

# PART 1
## WEIGHING UP THE RISKS

# WEIGHING UP THE RISKS

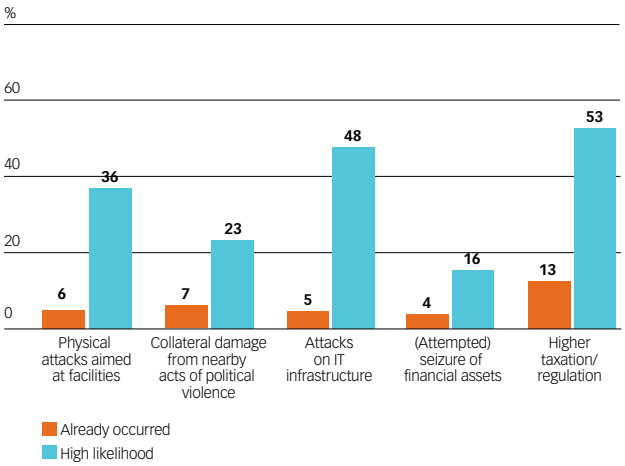
Companies believe they are operating in an increasingly dangerous world. The research reveals significant concerns among business leaders about the threat of terrorism and other forms of political violence, and how these issues might have an impact on their organisations.

For the growing number of companies operating on a global basis, the risk of being caught up in political violence is very real. Roughly one-fifth of firms in the survey have either already suffered direct physical attacks in their home market, or believe such an attack is very likely. A similar number have either suffered an attack overseas or think an attack is very likely. Moreover, these numbers are significantly higher among larger firms in the survey.

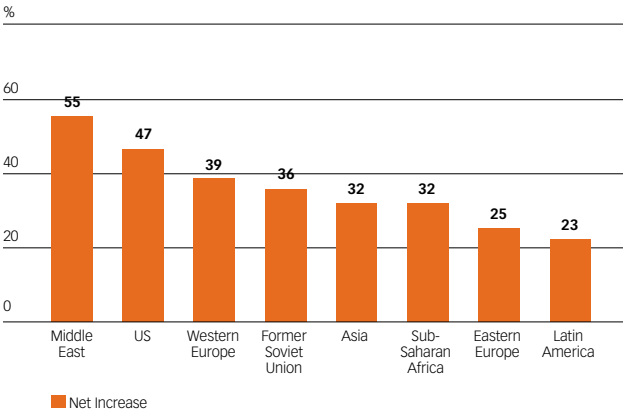
Three in five executives predict that the business risks associated with political violence will increase over the next five years, with the Middle East and the US seen as the two most affected regions. Perceptions of risk in a particular region tend to be higher among those who are based there. For example, 47% of Asian respondents predict rising violence in that region, compared with 36% of executives based elsewhere. The range of places cited by respondents as being potential sources of increased risk demonstrates the diversity of forms that political violence can take, and therefore the difficulty of addressing such violence. For example, the Middle East is no stranger to jihadi terrorism, local revolutionary movements, inter-state wars or complex amalgams of all three; the primary concern within the US itself is more specifically terrorism, particularly a repeat of 9/11; and various South Asian territories face ongoing efforts by nationalist or leftist groups to destabilise the state.

**"THREE IN FIVE EXECUTIVES PREDICT THAT THE BUSINESS RISKS ASSOCIATED WITH POLITICAL VIOLENCE WILL INCREASE IN THE COMING YEARS."**

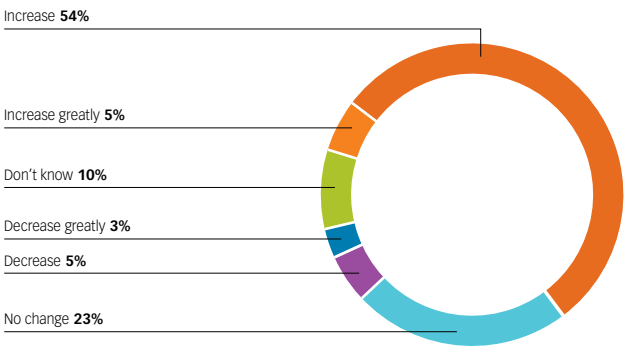
### What would you say is the likelihood that the following events will affect your business in the next five years?




### Over the next five years, how do you think the risk to your company of political violence/terrorist activity will change in the following countries/regions?

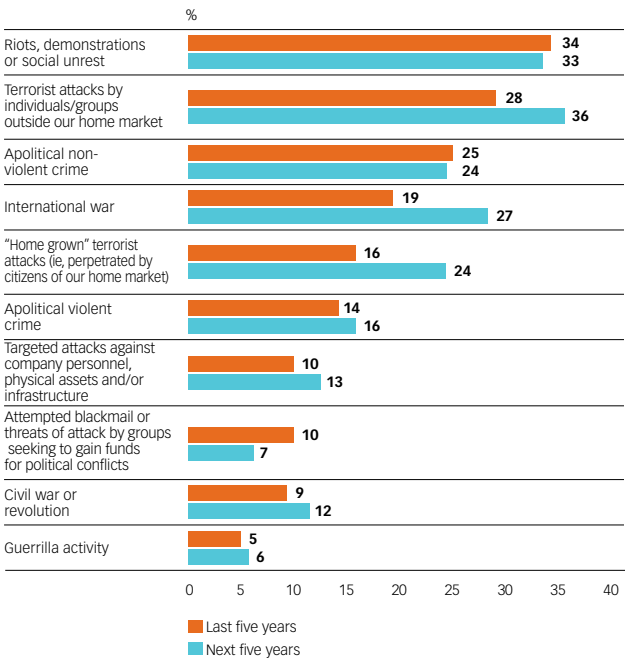



### Over the next five years, how do you think the risk to your company of political violence/terrorist activity will change worldwide?

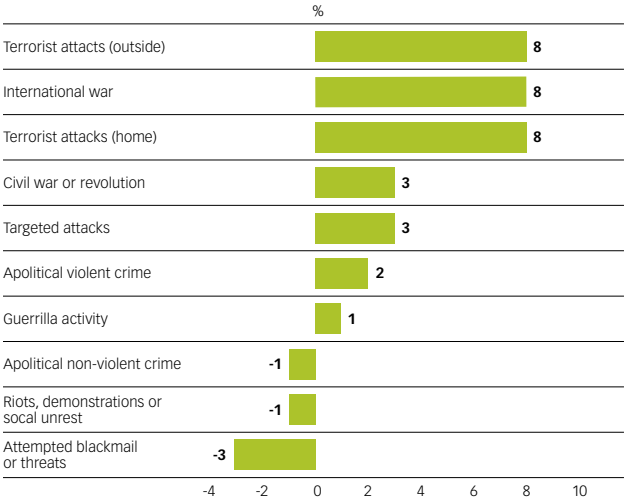


Companies also foresee a shift in the sources of violence, with international war and terrorism and home-grown terrorism the rising concerns, overtaking non-violent crime. On the one hand, concern over the impact of social unrest or riots is high but stable: for 34% of companies it was a top issue for the last five years, whereas 33% cite it as the top issue for the next five years. Likewise, concern about general criminal activity is stable. On the other hand, international terrorism is rising to become the single greatest concern for 36% of respondents over the next five years, up from 28% over the last five years. Similarly, international war is rising as a concern for 27% (up from 19%) and home-grown terrorism for 24% (from 16%). International terrorism is cited as a particular concern for US organisations and for large companies globally.

**Which of these do you think will present the highest risk to your company's operations over the last five years - and the next five years ?**



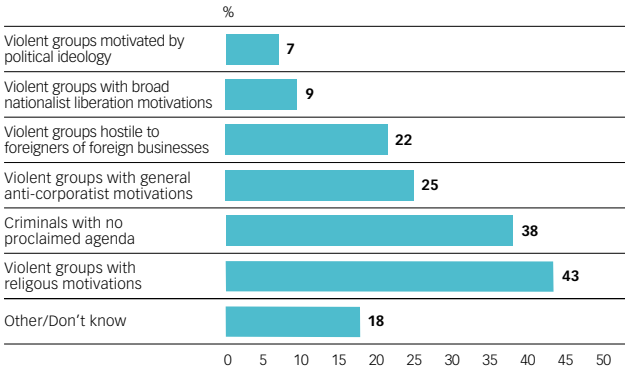

**Perceived top risks: Percentage point changes: last vs next five years**



# "THE MAJORITY, SOME 56%, BELIEVE THAT BUSINESS IS AS MUCH AT RISK FROM TERRORISM AS GOVERNMENT."

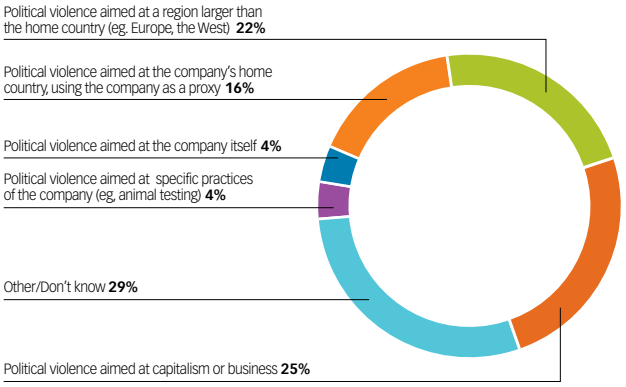
When asked who they feel most threatened by, businesses focus most on extremist religious groups such as Al-Qaeda and other jihadi terrorists. Anti-capitalist and anti-foreign groups are also cited as a threat, but perceptions vary by region. One-half of European respondents believe that ordinary criminals present the greatest threat, whereas 32% fear religious extremists and just 18% worry about anti-capitalists. Driven most likely by 9/11 and ongoing difficulties in Iraq, the figures are reversed in North America: 59% see religious extremists as a high risk, whereas 34% cite anti-capitalists and just 29% cite ordinary criminals.

**Which of the following groups do you think are most likely to pose the greatest threat to your business over the next five years?**




We also asked executives why the business community might be targeted specifically. Survey respondents from all regions believe they are targeted by violent groups because of issues over which they have little control. Only 8% feel that attacks are actually directed at the company or its practices. 16% feel that their firm's home country is the reason for attacks (27% from North America), 22% think it is the broader region, and 25% think it is capitalism as a whole. Almost one-third could not say why such attacks happen. Tellingly, 63% agree that companies face violence more because of what they are associated with than what they do themselves; indeed 23% think that suffering violence as a result of their home government's policy is a serious risk. But lack of responsibility does nothing to reduce their convenience as targets. The majority, some 56%, believe that business is as much at risk from terrorism as governments.

**Which of the following do you think is the greatest threat to your company?**




Despite some very real concerns, it is important to put things in perspective. Almost 45% of respondents believe that media and public discussion of terrorism paints a bleaker picture than their own experience suggests, compared with 17% who disagree. Business leaders are more worried about the impact of a disease pandemic on their supply chains than a terrorist attack (although North Americans are an exception here). The majority of companies do not think that a direct attack on their facilities and personnel is very likely. Instead, they show greater concern about the likelihood of non-violent political and security risks, such as contract frustration in difficult regimes (38% of firms), attacks on corporate IT infrastructure (53%), or the risk of taxes and regulation impeding operations (66%).

# "DESPITE EVENTS IN IRAQ, BY MOST MEASURES POLITICAL VIOLENCE IS ACTUALLY DECREASING."

## REALITY CHECK

Executives believe that the threat of political violence against business is growing, but is this grounded in fact?

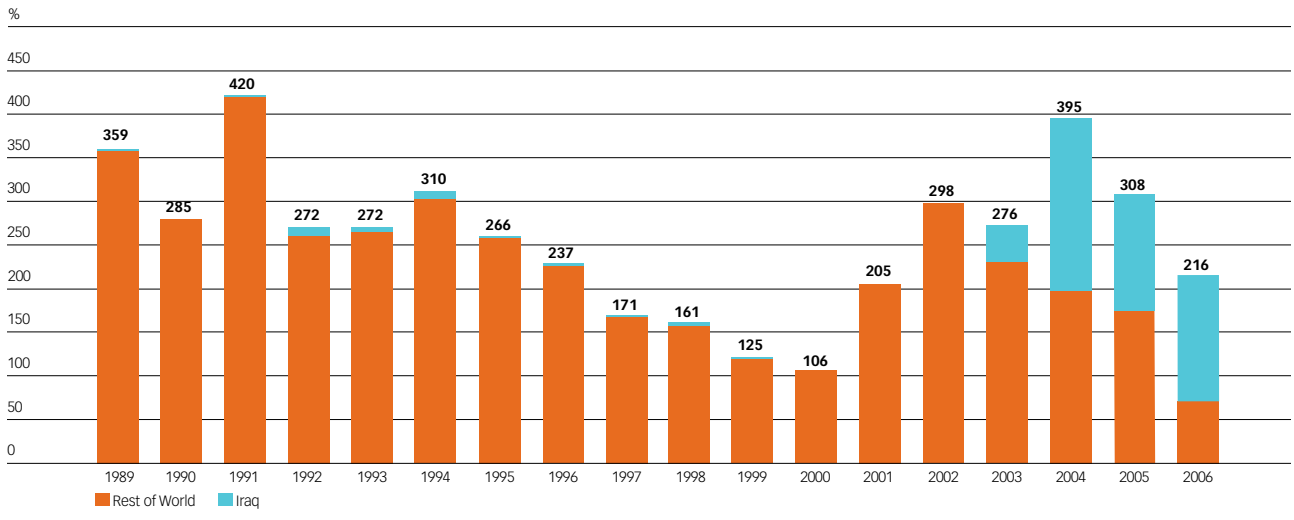
Despite events in Iraq, by most measures political violence is actually decreasing. For example, the 2005 addition of the *Human Security Report*, produced by the Human Security Centre at the University of British Columbia, and its 2006 supplement indicate a steady decline in the number of wars worldwide – from roughly 50 in the early 1990s to about 30 today – as well as a reduction in war deaths and genocides. Other sources give different statistics but the consensus is clear that the majority of conflicts are not the international wars that companies predict will rise, but rather more local conflicts.

Terrorism has also been decreasing in frequency everywhere except Iraq – where the distinction between civil war and a collection of terrorist actions is growing increasingly blurred. The Memorial Institute for the Prevention of Terrorism (MIPT, a US non-profit think tank) keeps the largest database of worldwide terrorist attacks. In the first half of the 1990s – the early post-Cold War period – the MIPT's annual figure for international terrorist incidents was in the high 200s, and peaked at 420 in 1991. Thereafter, it declined until 2000, which saw just 106 incidents. Since then, the figure has returned to the high 200s. However, it is notable that if attacks from Iraq are not included, the annual figures are in the low 100s, so actually below historical levels.

Domestic terrorism, where the perpetrator and the target are of the same nationality, follows a similar trend. It is usually linked to a local political struggle such as in Israel, Kashmir or Colombia. Outside of Iraq in particular, and of a handful of other countries to a lesser degree, the data reveals no evidence of an upsurge in terrorism.

It is also important to remember that most of these terrorist incidents are not directed against business. Roughly 20% of international terrorist attacks are against companies, according to MIPT data; the equivalent figure for domestic terrorism is around 7%. Since there are more domestic than international terrorist incidents, the number of such attacks against business is correspondingly higher. The incidents of domestic attacks on business vary between 150 to 200 per year with Iraq included, whereas international attacks on companies (excluding Iraqi activity) have dropped from around 50 annually down to the 30s. Balanced against this are three important facts: first, that a large number of "resolved" conflicts tend to relapse within five years; second, the number of "fragile states" has increased under Department for International Development and World Bank classifications; and third, jihadi terrorists have shown a particular interest in high casualty counts.

**International terrorist incidents 1989 - 2006**



# "AL QAEDA REMAINS A SERIOUS THREAT."

## NATURE OF THE THREAT

Executives see religious extremists as the most likely source of political violence. In reality, the picture is more complex. Self-described "Marxist" and nationalist terrorists were responsible for many more incidents than religious groups over the last six years, according to MIPT data.

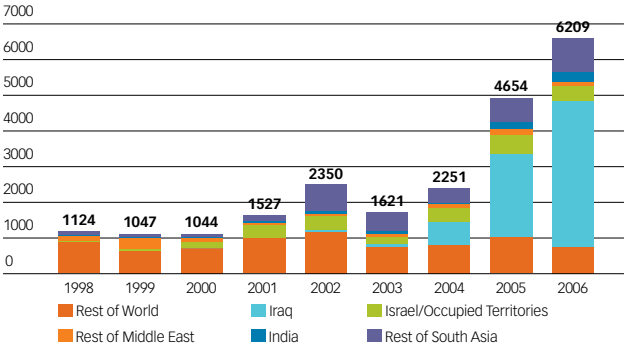
Companies may nevertheless be right to be more concerned by the religious extremist groups. Magnus Ranstorp, Research Director at Sweden's Centre for Asymmetric Threat and Terrorism Studies, and a leading authority on terrorism, believes that the jihadis are seeking to innovate in their approach to terrorism, which naturally poses new dangers.

Al-Qaeda remains a serious threat. Indications are that its leaders are able to exercise increasing freedom in tribal areas of Pakistan, and its record and pronouncements mean that its continued existence inevitably increases the risk of a further catastrophic attack taking place, despite some notable successes by law enforcement authorities in preventing others. Moreover, Al-Qaeda as an idea or "brand" is every bit as dangerous as the organisation itself. Its ability to encourage emulators, or even provide seed money and training for a very loose network of adherents, multiplies the threat many times over.

Professor Paul Pillar, now of Georgetown University and formerly one of the CIA's leading counterterrorism experts, also sees jihadi terrorism as the leading threat. This is especially so in Europe and North America, where it has already supplanted "leftist" terrorism.

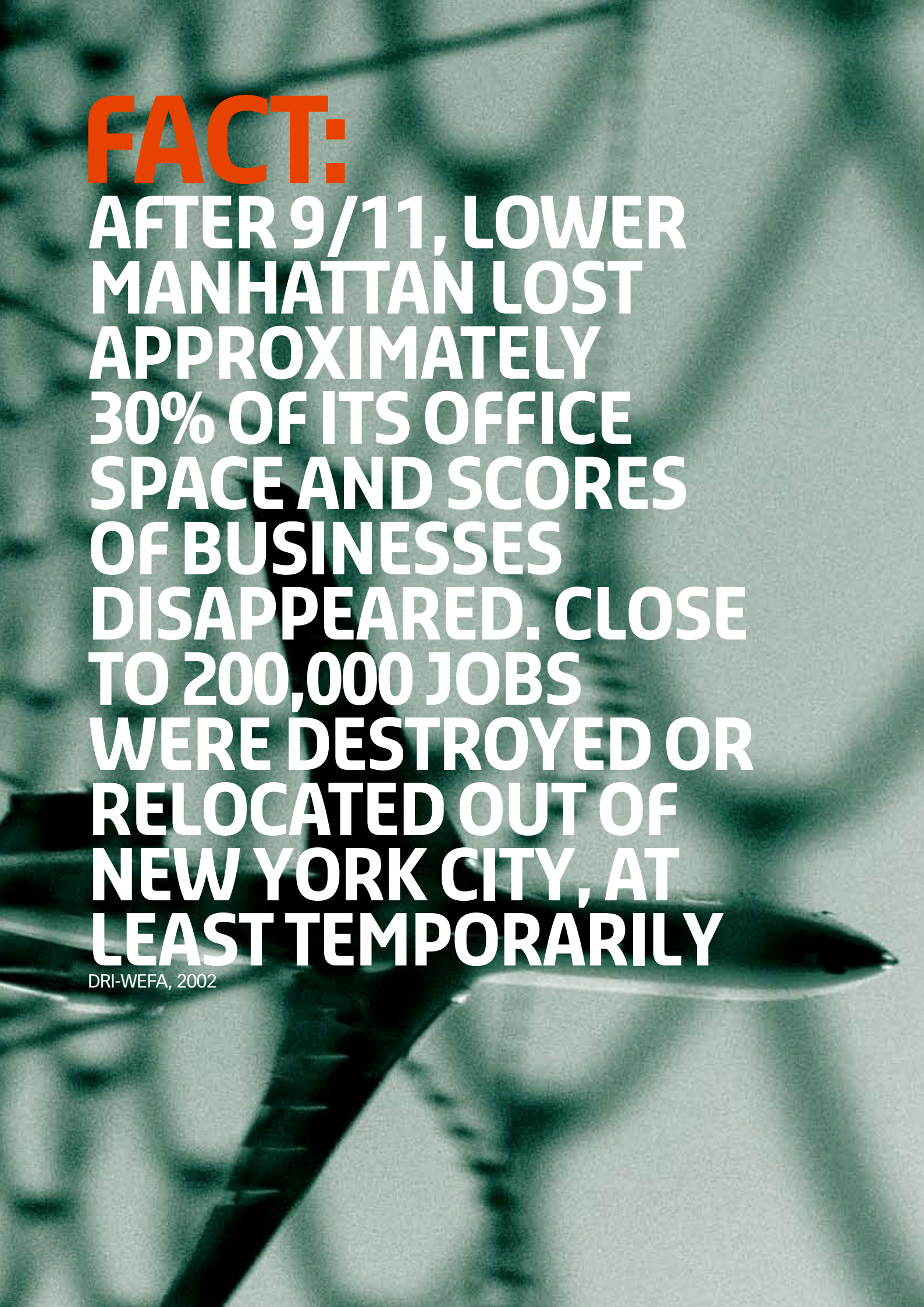
An increased threat from jihadi terrorists is obviously a concern, but it does not necessarily indicate a greater threat to business. Most attacks against business, whether domestic or international, have been by left-wing, nationalist, or issue-oriented groups. Professor Brian Jenkins of Pardee RAND Graduate School, another of the world's prime authorities in this field, believes that despite Al-Qaeda's talk about economic warfare, the "desire to run up high body counts is the most important criterion" in target selection. This fact militates against strikes being primarily directed against most business facilities, although certain sectors are more vulnerable than others as attacks on energy facilities and financial institutions prove. Of course, there is the possibility that another major attack could inflict simultaneous political and economic damage in the same strike.

**Domestic terrorist attacks by territory**




However, it can be argued that 9/11, which accounted for over one-quarter of all fatalities suffered in attacks on businesses over the last 40 years, gives a false impression of the typical threat to firms. A more representative example might be an act of domestic terrorism – often a small bomb – with few casualties. On average one person dies. As often as not, those attacking the company do not claim credit so they remain unknown. Mr Jenkins describes the risk of injury or death to employees from such activity as "infinitesimal". Adam Roscoe, Group Head of Sustainability Affairs at ABB with special responsibility for security, believes that his company's people are most likely to come under threat from criminals rather than terrorists. Mr Jenkins agrees: "The big personal security issue abroad is ordinary crime, particularly violent crime."

While these points help to put the threat of terrorism in context, there is little doubt, however, that we are living in a new era where terrorists seek to plan spectacular attacks that may not only have an impact on business directly, but also bring economic activity to a halt indirectly. Experts agree that there is no room for complacency, not least where misinformation abounds. Several analysts interviewed for this study note the difficulty of counteracting assumptions that jihadi terrorists are focused on Americans, not Europeans. Victor Meyer, Global Head of Corporate Security and Business Continuity at Deutsche Bank, points out that no countries are exempt from risk. For example, Germany has recently seen failed terror attacks. It is a sensitive issue, but one analyst points out off the record, "Terrorists rarely ask to see passports." Opinion and therefore risk levels can also turn quickly, as Danish companies abroad found during the cartoon crisis.



# FACT:

## AFTER 9/11, LOWER MANHATTAN LOST APPROXIMATELY 30% OF ITS OFFICE SPACE AND SCORES OF BUSINESSES DISAPPEARED. CLOSE TO 200,000 JOBS WERE DESTROYED OR RELOCATED OUT OF NEW YORK CITY, AT LEAST TEMPORARILY

DRI-WEFA, 2002

# "WHERE BUSINESSES ARE THE TARGET OF TERRORISM, IT IS USUALLY BECAUSE OF WHAT THEY REPRESENT, RATHER THAN ANYTHING THEY DO."

## WHY US?

Where businesses are the target of terrorism, it is usually because of what they represent, rather than anything they do or don't do themselves. Global brands can assume symbolic significance for terrorists. The US National Counterterrorism Center's list of significant terrorist events describes 24 attacks on McDonald's restaurants between 1993 and 2005 worldwide. Of the minority where responsibility was claimed, motivation for the attacks included nationalism, anti-globalisation, religion and Marxism – but in each case the perpetrators objected to the restaurant as a symbol of America, not a purveyor of products. Mr Jenkins notes that, before 9/11, the two best correlated predictors of whether a US firm would suffer an attack were size and familiarity to the public – corporate behaviour, even philanthropy, was inconsequential. Added to this is the very real possibility of risk displacement: business targets are often easier to hit than government facilities or sites.

Other forms of political violence may be more directly linked to the company's behaviour, especially in civil conflicts within weakly governed states. Jonny Gray, Head of Crisis and Security Consulting at Control Risks, a business risk consultancy, argues that a firm's level of risk is not just about symbolism. Rather, it is governed by "a complex, dynamic combination" of perceptions, the sector in which it operates, and how it interacts locally. "Companies, especially large ones, need to remain steadfastly apolitical, but conscious that they are actors nonetheless," he comments.

An awareness of the social, political and economic impacts that business operations can have on local environments is a crucial first step in effective risk management. Nick Killick is Manager, Peacebuilding Issues Programme, at International Alert, an NGO that promotes peace. He warns: "You can do all sorts of bad things with good intentions if you're getting into something you don't understand." The NGO community has useful insight in this area. In the past decade, many have engaged in soul-searching over the ways in which parties to conflict have hijacked well-intentioned humanitarian and development efforts to their own ends. Companies can either profit from others' experience or learn the hard way.

## AN UNPREDICTABLE FUTURE

Although statistics paint a picture of abating political violence, a shift towards increased risk is possible for a number of reasons.

First, terrorism does not follow simple statistical patterns. "The most difficult areas to predict violence are not conflict zones, but more developed areas of the world, where terrorists try to do a spectacular event in a well-ordered society," says Mr Roscoe. Worldwide, Al-Qaeda and its emulators either carry out or are caught before executing about one attack per month, some on a very large scale. Moreover, Osama bin Laden's speeches speak of his followers being justified in killing up to 4 million Westerners, 2 million of whom could be children. A series of large atrocities is not impossible.

Second, the long-term impact of the Iraq conflict on security could spread worldwide. Mr Pillar draws the analogy with the war against the Soviet occupation of Afghanistan, which, like Iraq today, "served as a training ground, networking opportunity and inspiration to jihadists". Mr Jenkins believes that Iraq may pose an even bigger threat, because terrorist experience gained there is more easily applied elsewhere (like the West, 70% of Iraq is urban, whereas much of Afghanistan is mountain wilderness).

"We are only seeing the beginning of potential blowback from Iraq, or even Somalia which is becoming equally dangerous," warns Mr Ranstorp. Most groups in normal times manage only a few operations per year, but Iraq is seeing over 100 per day, with groups exchanging knowledge between themselves. Tactics are being exported: British police recently arrested plotters allegedly aiming to kidnap and behead a soldier, which was presumably inspired by highly publicised terrorist practices in the Middle East. Mr Ranstorp also believes that there is a blurring of boundaries between Islamic, anti-globalisation, and anti-American groups, with "hatred of the United States in all its manifestations causing these to move in the same direction".

# "OTHER EMERGING RISKS SUCH AS CLIMATE CHANGE AND INCREASED SHORTAGES IN NATURAL RESOURCES ARE LIKELY TO MAGNIFY THE THREAT OF POLITICAL VIOLENCE."

Terrorist groups with different causes and motivations have always exchanged knowledge – for example the collaboration between the Irish Republican Army (IRA) and Spain's ETA, or with the Revolutionary Armed Forces of Colombia (FARC). Each new generation of terrorists looks to previous ones for operational models and inspiration. Today's jihadists are the benchmark of future terrorism, whatever its ideology, according to Mr Jenkins. Modern communication technology must also be taken into account, given that it makes it much easier for these groups to share information.

Like terrorism, war will also continue to change. "Instead of nation states, we have insurgents, terrorist and militias," notes Mr Meyer. These civil wars that involve a multitude of small, shifting groups rather than clearly defined sides pose large challenges for business, beyond simply their greater unpredictability.

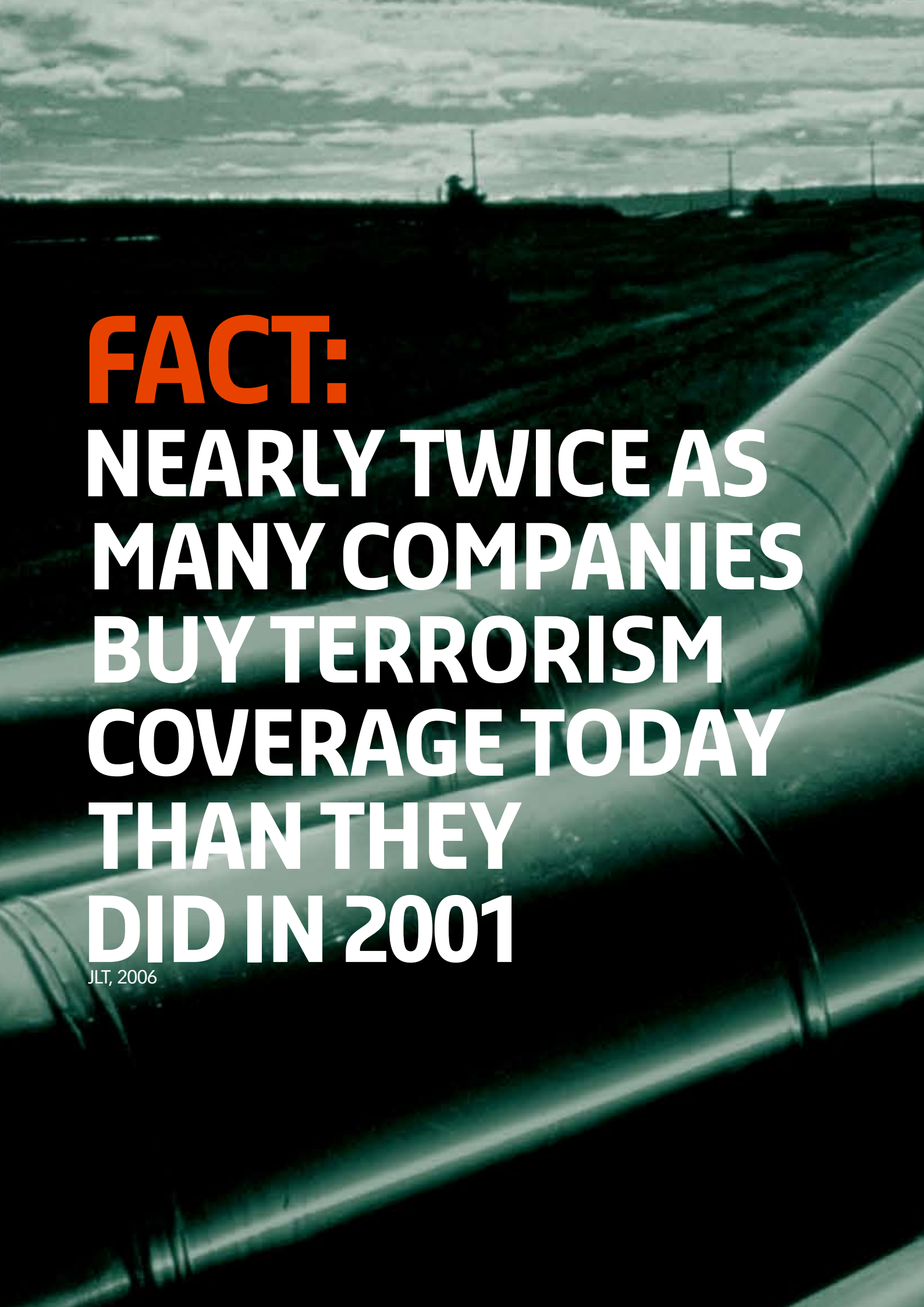
The type of combatants in the more amorphous wars also creates new dilemmas. Amanda Gardiner, Programme Manager at the International Business Leaders Forum (IBLF), says companies can now face small, unstable militias – bigger than criminal gangs, smaller and less disciplined than armies – controlling areas where they operate. Somalia, Uganda, Afghanistan and the Democratic Republic of the Congo all provide recent examples. Learning how to deal with these situations will take many companies into unchartered territory.

Another challenge for businesses is that the international community is watching corporate behaviour more closely in zones of weak governance, bringing reputational considerations to the fore. Active divestment campaigns in respect of certain regimes are one example of this. "The concept of complicity in human rights abuses and related issues has grown," comments Edward Bickham, Executive Vice President, External Affairs, at Anglo American. "Expectations and accountability for indirect impacts are also growing. That evolving backdrop – which will vary between countries – clearly creates reputational risks, if you misread where those expectations are or their trajectory." Several companies have also been found responsible for having benefited from poor labour standards in conflict zones and being engaged in improper acquisition of assets and association with repressive governments through royalty payments. And it is no longer just public opinion where companies can fall foul. According to the International Committee of the Red Cross, business executives can face charges under war crimes statutes for actions of local managers.

National courts also pose concerns. "Case law is beginning to show that if you could reasonably foresee an event involving political violence but have not managed that risk, then board members may be individually liable," notes Mr Gray. Another analyst says privately, but more bluntly: "A lot of what drives security policy is fear of what would happen if a company is hauled across the coals in a US court."This could be by zealous district attorneys or, increasingly, by NGOs using the Alien Tort Statute (ATS) to sue. A recent ruling held that a corporation can be held liable under the ATS where a corporation has aided and abetted abuses or where members of the military act on behalf of the corporation in committing abuse.

Finally, other emerging risks such as climate change and increased shortages in natural resources are likely to magnify the threat of political violence. Conflicts frequently revolve around the division of a state's natural resources, making companies involved in their use inevitable targets. A widely-predicted increase in resource wars, particularly over water, energy and arable land in the wake of global warming, could increase this difficulty, especially where natural resource management has been poor. Some recent conflicts – for example, Darfur – have certainly been exacerbated by climate-related factors. Boutros-Boutros Ghali, himself Egyptian, has said that "the next war in the Nile Region will be fought over water, not politics." While it is difficult to predict how climate change might trigger increased political violence with any certainty, it is clear that these issues can only add to the complexity of the overall risk environment.

# PART 2
## CORPORATE RESPONSE



# FACT:

# NEARLY TWICE AS MANY COMPANIES BUY TERRORISM COVERAGE TODAY THAN THEY DID IN 2001

JLT, 2006

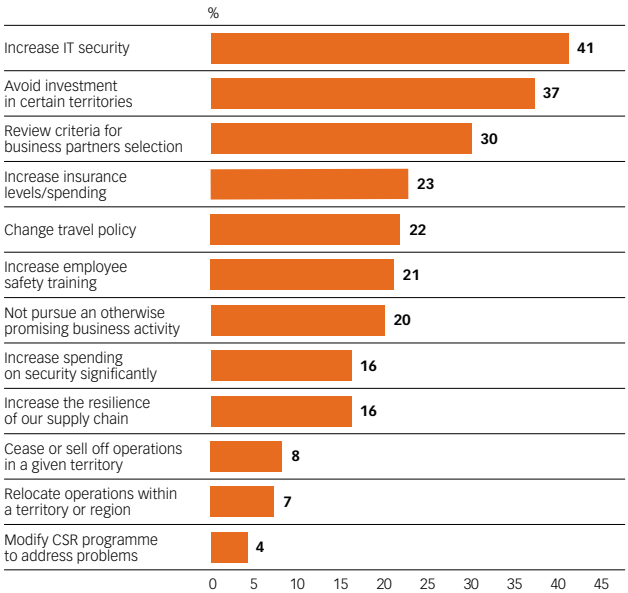
# "SMALLER COMPANIES SHOULD NOT BE UNDER AN ILLUSION THAT THEIR SIZE MAKES THEM LESS VULNERABLE."

The risks associated with terrorism and conflict, whether real or perceived, are sufficiently high to cause many companies to take action. Political violence has, in the last five years, led:

- 41% of respondents to increase IT security
- 30% to review business partner selection criteria
- 23% to augment insurance spending
- 21% to increase employee safety training

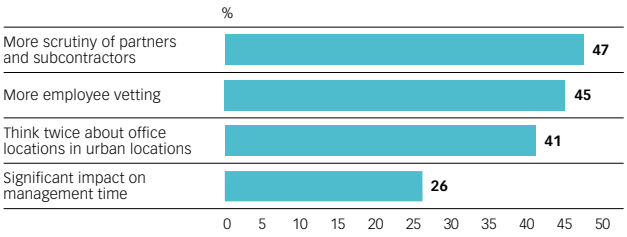
Larger companies in the survey are the most likely to take action. A majority, 60%, have adjusted their continuity plans, 40% have increased safety training and reviewed partner selection criteria, and 26% have raised security spending significantly. Smaller companies should not be under an illusion that their size makes them less vulnerable, however. They are no less likely than larger organisations to be caught up in collateral damage from a terrorist attack or outbreak of violence, for example.

**In the last five years, has political violence (including terrorism) led your company to do any of the following?**




Home-grown terrorism poses a particular challenge that may require additional measures, particularly in Europe, where the traditional terrorist threat from separatists is no longer the only home-grown threat, and the rise of European national jihadis seems to have taken society by surprise. 26% of all firms, and 40% of large companies, agree that employee anxiety about this risk has a significant impact on management time and decision-making. More than 40% of business leaders now think twice about putting key offices in major urban locations, and 45% vet employees more carefully. Among European companies, 36% now think twice about putting facilities in major urban locations, and 49% vet employees more carefully. The cost of management time to deal with home-grown terrorism is difficult to quantify, but the financial impact must be significant.

**Recent terrorist attacks have highlighted the risks associated with 'home-grown' Islamic extremist terrorism in some countries. How is your company responding?**

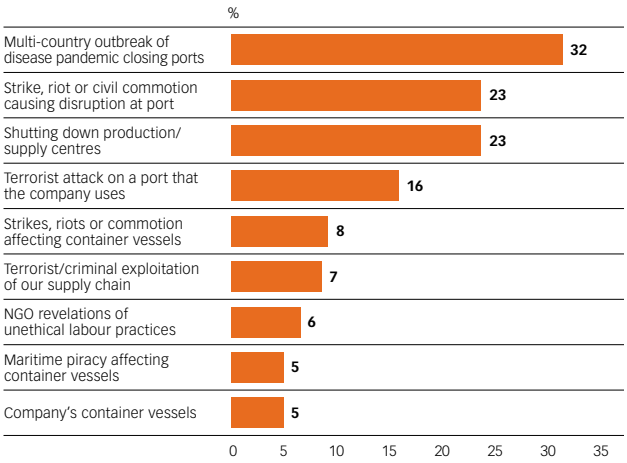


Supply chain management is another risk that is emerging as a greater concern. The most forward-thinking companies are taking steps to protect their increasingly global supply chains specifically against the potential impact of political violence. 16% of all firms, and 24% of large ones, have tried to strengthen their supply chain resilience in response to an array of supply chain risks, with the two most commonly cited being the impact of civil unrest on suppliers' ports and direct terrorist attacks on their own facilities. This seems an appropriate response: in February 2007, Al-Qaeda called for attacks on all US oil supplies as a component of economic jihad, although this has yet to occur in practice. There have also been repeated attacks in the Niger Delta and Saudi Arabia as militant groups come to appreciate their ability to affect oil prices.

Increased attention in this area is sensible, but should not be restricted to a focus on the company's own supply chain. According to Mr Jenkins of Pardee RAND Graduate School, a company is far more likely to face the broader impact of a catastrophic attack than to be the direct target. Enhanced supply chain resilience should therefore emphasise alternate routes for obtaining vital supplies, rather than simply protecting facilities. The majority of companies are currently failing to build supply chain issues adequately, into their risk management thinking. In an increasingly interconnected and outsourced economy, understanding and protecting the supply chain will become more important to business continuity.

**"THE MOST AWARE COMPANIES ARE TAKING STEPS TO PROTECT THEIR INCREASINGLY GLOBAL SUPPLY CHAINS SPECIFICALLY AGAINST POLITICAL VIOLENCE."**

**Which of the following supply chain risks do you think pose the greatest threat to your business?**




While it is clear that companies are spending more time and money on managing the numerous risks associated with political violence, the biggest cost of all may not relate to what companies do in response, but rather to the opportunity cost of what they don't do. For many companies, these risks have a significant impact on their investment decisions, and therefore potentially on company growth and development. Thus 37% of companies in the survey say that the risk of political violence has led them to avoid investment in certain territories over the last five years. Similarly, one in five say they have decided not to pursue a promising opportunity because of concerns about exposure to political violence. This reflects the experience of a number of African countries, for example. In the Côte d'Ivoire, recent political unrest, including rioting and threats against foreigners, led the African Development Bank and a number of foreign businesses to relocate. Political violence has also caused a number of firms to divest from Nigeria. But with appetite for cross-border investment growing in developing markets, it is clear that if companies in developed markets are not prepared to invest, they could lose out to others that are.


## COMPUTERS AND TERRORISM: WHAT'S THE WORRY?

When asked what action they have taken in response to the risk of political violence, companies in the survey are most likely to refer to increased computer security. As many as 40% of all firms and 55% of large companies say they have raised IT security spending to confront these threats.

There is no doubt that today's violent groups are adept at using IT for communication and networking, and that some of them use online sources to market their cause or to recruit and train members. However this kind of activity must be distinguished from an attack that is designed to disrupt or damage the victims' IT networks.

There are some politically motivated hackers who have defaced websites or launched Denial of Service attacks on corporate IT systems. These cyber-rimes are potentially expensive, but they are much more likely to be initiated by ordinary hackers.

Usually the definition of cyber-terrorism is restricted to infiltration of IT systems to damage whatever they control. There are two schools of thought on this risk: those who see it as a growing, significant danger and those who consider it largely hype. The former stress the increasing interconnectedness of computer networks, the IT competence of terrorist groups, and some evidence indicating that some of these groups, including Al-Qaeda, have shown an interest in the potential of such attacks.

Sceptics point out that IT infrastructures and defences are robust enough to cope with most cyber-threats. Moreover, terrorists – especially jihadi ones – tend to seek out more dramatic, media-grabbing acts of violence rather than the disruption of IT systems. Certainly, examples of cyber-terrorism are extremely thin on the ground. In July 2005 the FBI's Cyber Division said it knew of no significant electronic terrorist attacks against the US government, which is likely to be the biggest target for any cyber-terrorist. By contrast, the Pentagon alone saw 160,000 attacks by hackers on its computer system in 2005.

Nevertheless, at least a few incidents do raise eyebrows. Gary McKinnon, a British hacker, ostensibly looking for suppressed evidence of UFOs in 2001 and 2002, now faces trial in America for, amongst other things, causing US$700,000 dollars worth of damage to US government computers and shutting down a naval weapons station's IT systems for a week.

Lack of cases so far has certainly not stopped spending. The US government has appointed its own cyber-terrorism czar and spent billions on infrastructure security over the years. Similarly, there is an argument that business should be prepared. Computer attacks that cause large-scale power outages or stop trading could certainly bring a business to its knees. Mr Meyer of Deutsche Bank sees a similar dynamic to Y2K risk. "Why has there not been a catastrophic attack on the Internet's root servers – is the threat not there, or are we one step ahead?" Whatever his doubts about the real dangers, he concedes that "it would be irresponsible to assume the threat is non-existent. We simply have to address it in a disciplined way."

The link between IT security and terrorism is important on several other levels. First, as noted, many terrorist organisations are avid and adept users of information technology. This has allowed the creation of highly dispersed organisations and networks that are extremely difficult to break up completely. Second, criminal operations usually fund terrorist activity, so terrorist groups are yet another set of actors who might see cyber-crime as a highly profitable way to secure the funds they seek, or use networks to move and launder money surreptitiously. This type of criminality would not change the nature of the threat IT systems face from cyber-criminals, but could certainly add to the volume.

Overall, there are a host of good reasons to invest in IT security. Terrorists and other violent groups may not alter significantly the kind of risks faced or solutions needed, but they add to the urgency of the problem.

# "ONLY 36% HAVE A STRONG UNDERSTANDING OF THEIR EXPOSURE TO POLITICAL VIOLENCE."

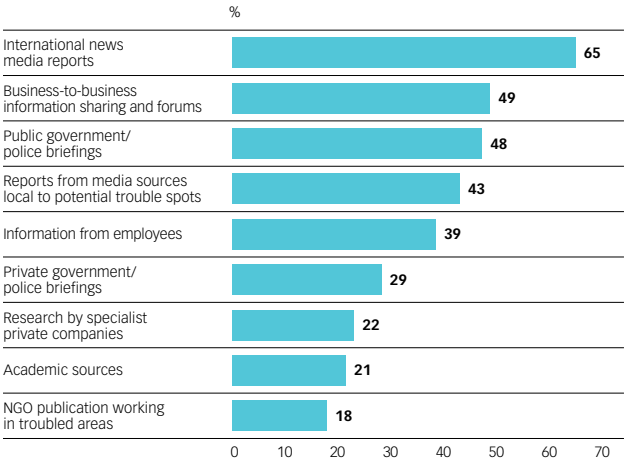
## TOO MUCH INSTINCT, NOT ENOUGH INSIGHT

Companies are devoting substantial resources to mitigate the risks of political violence. They are also foregoing significant business opportunities. They are not, however, always investing their time and resources in the right places. The main reason seems to be that they are not doing enough to analyse and understand the real risks against their business. 10% of firms surveyed do not bother to gather relevant information, and only 36% have a strong understanding of their exposure to political violence. The case for more work in this area can be widely made, not least because companies that fail to show sufficient due diligence in conducting pre-investment risk assessments, could face extraterritorial legal challenges.

Thorough analysis is particularly important for this category of risk because companies may find the underlying dynamics unfamiliar. Ed Potter, Director of Global Labour Relations and Workplace Accountability at Coca-Cola, believes that working in zones of conflict requires a special approach to analysis. "You have to think about problems somewhat differently, in part to understand why the situation is as it is," he comments.

What seems to be lacking for most companies is any kind of co-ordinated strategy for information gathering. Most companies (65%) rely on international media as a source of information on political risks. This is a sensible start, points out Mr Bickham of Anglo American, particularly for timely, breaking information. But too few go any further. Only 43% use local media in troubled areas, despite the fact that the Internet makes these as easy to access as international publications. Fewer than half engage in business-to-business information sharing or use public government briefings. Only about one-fifth of companies seek out specialist information, such as specialist private research, academic writings or NGO reports. All three can be of extremely high quality; the latter two are often free. Most worrying, only 39% have a mechanism for employees to feed information they have learned into political risk analysis, yet someone working long term in a strife-torn country will often have a better sense of changing risks than international reporters who jet in and out.

**Which information sources does your company use to gather data on risk associated with political violence?**




Best practice is not a case of using one or other of these tools. Both Mr Bickham and Mr Roscoe of ABB say their companies regularly use almost all these sources. Mr Potter refers to Coca-Cola "knitting together" information for a range of sources, including labour unions, which have just as strong an interest as companies in worker safety. Mr Meyer is surprised by how few companies make full use of these information sources. He cites Crowe's Law – "Do not believe what you want to believe until you know what you ought to know" – as an important guiding principle when dealing with political risk. In some very important cases, Deutsche Bank deploys people to monitor possible early warning indicators that other sources are not covering.

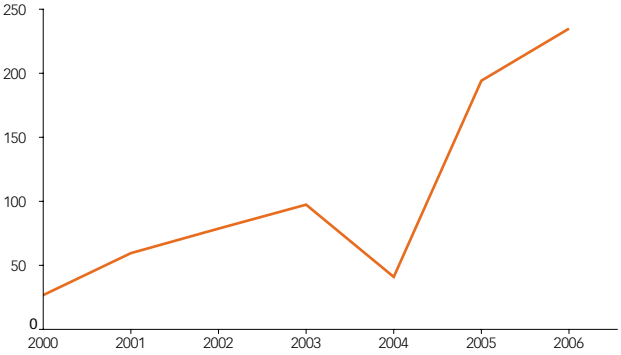
This knowledge can do more than improve the accuracy of risk assessments. "The challenge for the best companies now is to move from being reactive, and to turn an acute understanding of risk to commercial advantage," says Mr Gray of Control Risks.

# "ANOTHER PROBLEM IS MANY COMPANIES REMAIN RELUCTANT TO EXCHANGE INFORMATION."

Radmilla Sekerinska is the leader of Macedonia's largest opposition party and former acting prime minister. She was already a leading politician in 2001 when ethnic fighting shook the country, and has learned a lot about how companies engage with the issues of political violence. She notes that, in Macedonia's case, most foreign companies just know what they learn from CNN, the BBC and The Economist, which publishes an article on the country "every two years". However, the more successful foreign firms investing in Macedonia are those that gather information and insights from people on the ground, particularly peers who preceded them, in order to get a better idea about the real risks and opportunities. Indeed, she notes the irony that the more informed companies do not fully trust the international media to provide an accurate and complete assessment of the issues relating to these markets.

Several factors might explain why so few companies fail to undertake full analysis of these issues. First, although companies believe that the threat of political violence is increasing, they do not always link this with their own operations. This is a mistake. Large numbers of Western companies are investing into India's booming economy, but not all of them fully appreciate the risks of political violence in that country. Between 2000 and 2006, the annual number of terrorist attacks grew steadily from 26 to 235 – and that is not including Kashmir, where activity has been far greater. Ongoing guerrilla or terrorist movements in the north-western, north-eastern, and eastern provinces of India remain headaches for the authorities.

**Terrorist incidents in India (excluding Kashmir): 2000 – 2006**




India is not the only example. "The increase of business in emerging markets will increase exposure theoretically; it brings the developed and developing world in contact," explains Mr Meyer. Larger companies understand this better and have become more sophisticated in their approach. They are far more likely than smaller counterparts to use specialist or academic research and to exchange private information with governments. By comparison, many smaller firms operating abroad lack knowledge of local conditions, according to Mr Jenkins. Worryingly, despite less effort to analyse risks in this area, smaller companies in the survey were far more confident that they understood the risks of political violence than larger companies.

Another problem is that many companies remain reluctant to exchange information on these issues. Many companies, for example, refuse to discuss security publicly because, they contend, doing so would make them less secure.

Mr Meyer used to agree, but now thinks it's a "huge error" not to talk about it, precisely because rapid information exchange between all interested parties has become essential to security. This includes the exchange of information internally. By involving staff in security solutions, companies help to create a culture of security awareness and resilience that is ultimately a more effective and less costly way to protect their assets.

Mr Jenkins believes that governments have also been too slow to shed a constraining Cold War security culture for one that emphasises rapid intelligence dissemination. Opportunities for closer public-private sector interaction on the issue are clear, and the UK Treasury is an example of one government ministry that is actively promoting this.

Ms Gardiner of the IBLF points to mistrust between business and pressure groups as one reason that only 13% of large corporations report that they use NGO information. However, companies soon learn when things go wrong. "Continuing mistrust between business and NGOs cuts off the potential for a useful exchange of knowledge and intelligence on both sides", she says "One trend IBLF sees is that companies are starting to recognise that NGOs can effectively play a dual role of both constructive critic and collaborator, particularly when mutual goals are at stake."

# FACT:

## 15 COUNTRIES POSE LESS OF A RISK IN 2007 COMPARED TO 2006, CONTRIBUTING TO A DECREASE IN THE OVERALL LEVEL OF GLOBAL POLITICAL RISK FOR THE FIRST TIME IN THREE YEARS

Aon Political and Economic Risk Map, 2007

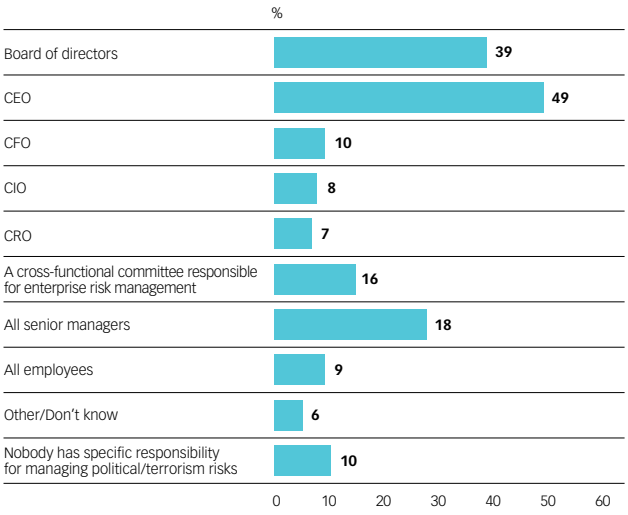
Although information exchanges are now more common between companies and NGOs, they do not extend far enough, according to Mr Killick of International Alert. Everyone stands to lose if communication is not improved. Mr Bickham and Ms Gardiner, from opposite sides of the divide, believe that one of the great benefits of participation in the Voluntary Principles on Security and Human Rights scheme has been the corporate-NGO exchanges that did not occur a decade ago. Time will tell whether this will lead to the development of a set of governance and accountability criteria that will be supported by companies and NGOs alike.

## RISK MITIGATION STRATEGIES

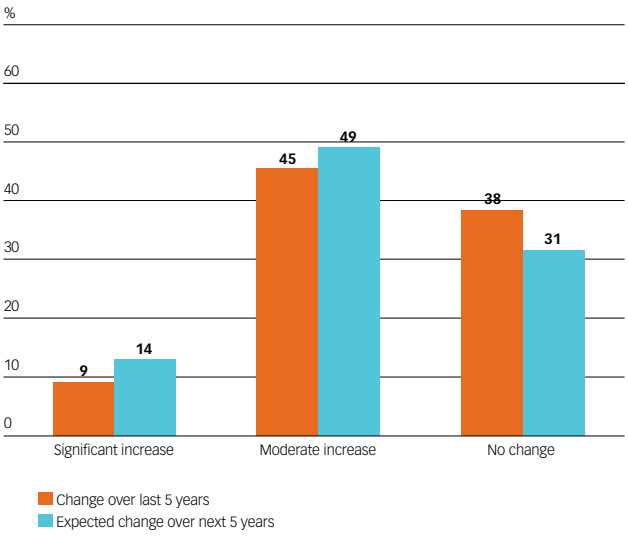
The majority of boards are spending more time considering these issues than they did five years ago, and over 60% believe that this trend will continue over the next five years too. But in addition to learning more about risks surrounding political violence, the majority of companies in the survey could do a lot more to reduce their potential exposure to what most agree is a broad issue that is likely to grow in importance.

No blanket prescription covers all companies. Successful companies address security in different ways – some in a stand-alone function, others through committees, still others within functions such as human resources or corporate social responsibility. Mr Gray distinguishes between a hypothetical large extractive company operating in troubled regions and a small, Scandinavian advertising firm. Each would obviously devote different resources to protecting their business. Nevertheless, some steps make sense for everyone. The first is the recognition that the risk exists. As mentioned earlier, 10% of firms do not collect information on political violence risks. Worse still, 22% do not address these risks systematically, even within broad risk management strategies.

**Who at your company is responsible for monitoring and managing risks associated with terrorism and political risk? Select all that apply.**




**In your view, how is the amount of time devoted by your board to the discussion of terrorism and political risk changing?**

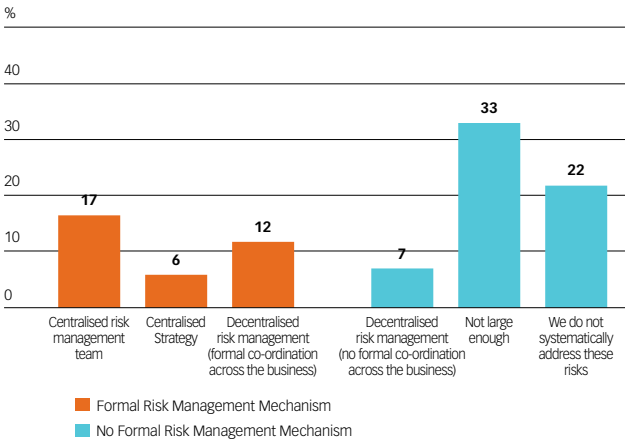


# "NEARLY ONE IN FOUR COMPANIES HAVE NO BUSINESS CONTINUITY PLAN AT ALL, AND A FURTHER 14% SAY THEIR PLAN IS INSUFFICIENT IN LIGHT OF CURRENT POLITICAL VIOLENCE."

Another vital step is to build the risk of terrorism or political violence into the business continuity plan. This assumes, of course, that the company has one in the first place. In fact, in the survey, nearly one in four companies (23%) do not have a business continuity plan at all, and a further 14% say that their plan is insufficient in the light of current political violence challenges.

This problem is particularly marked among smaller firms, where almost one-half (49%) need a new or improved plan. A surprisingly large number of companies are overlooking one of the first building blocks of risk management strategy. Failure to develop a robust continuity plan is rather like not running fire drills. Mr Roscoe of ABB believes that the most important criteria for operating in a potentially dangerous place is to ensure that all the people who go into a territory understand the risk and the contingency plans.

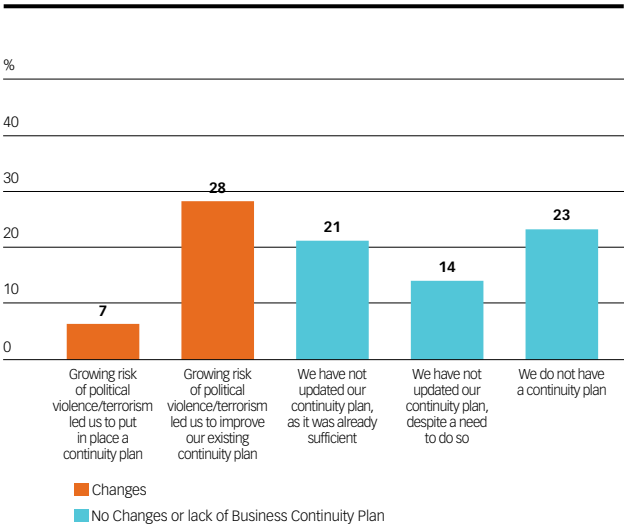
**How does your company manage the risks of political violence?**

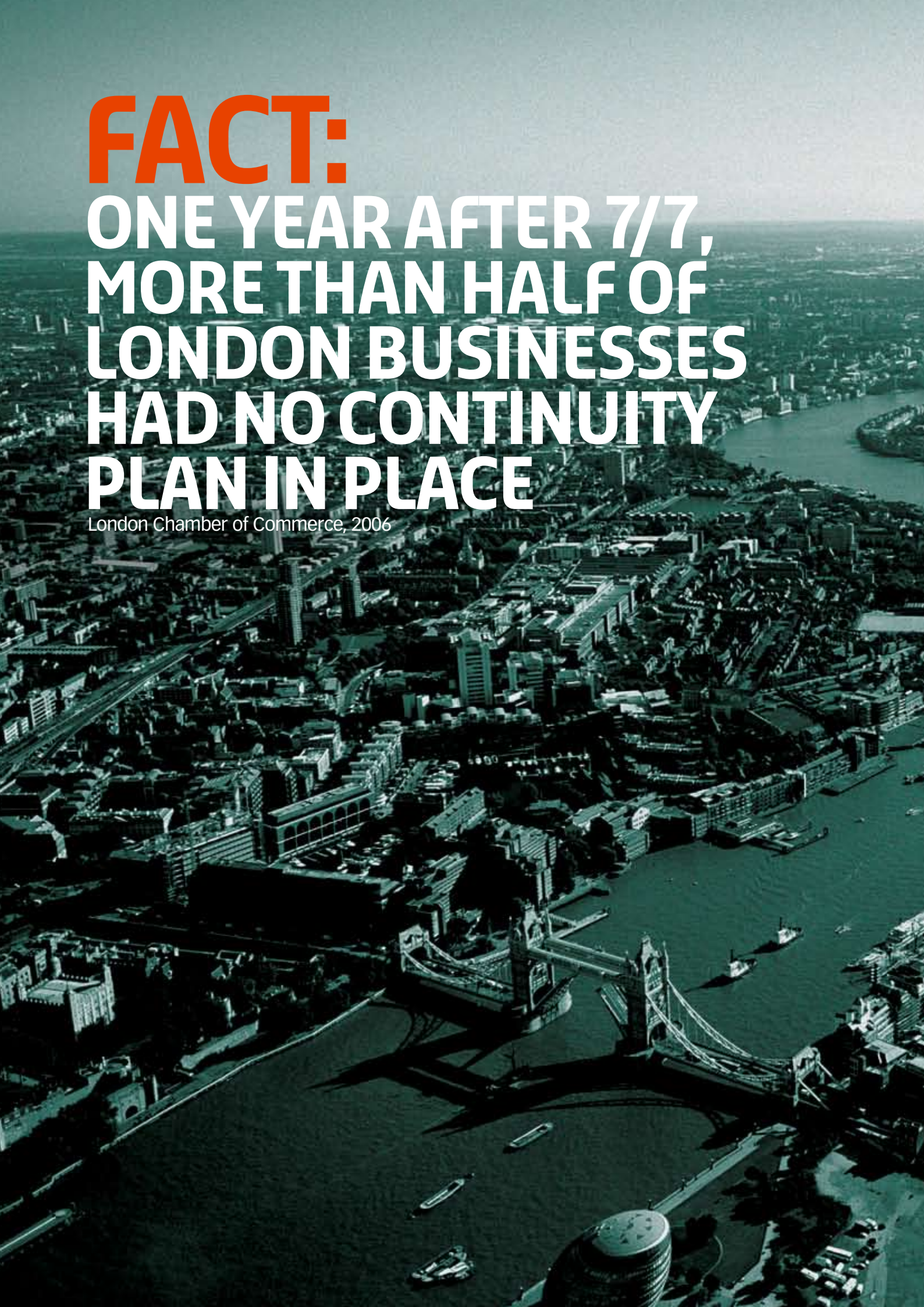



Moreover, existing plans may not go far enough. Only 20% of companies surveyed cover a chemical, biological, nuclear or radiological attack in their plans (31% for larger companies). In the last five years, in both France and the UK, plots to engage in widespread ricin poisoning have been foiled by police. Prudence, not alarmism, should encourage closer consideration of the risk of such attacks, especially where the technology for them exists, as in the case of dirty bombs. Evidence suggests that Al-Qaeda has great interest in such weapons, although it would be alarmist to suggest that the threat is imminent.

Another problem is that the corporate approach towards terrorism and political violence risk seems to lack consistency. When asked how their companies would respond to another highly public terrorist incident in the future, most feel that they would experience a short-term heightening of security, which would fade out or become inconsistent relatively quickly. As Mr Gray puts it, "people have short memories", and security has more to do with the nature of the business than experience. Mr Meyer believes that the key is to turn security issues into "sticky" ideas – ones that people can keep in mind.

**Which best describes changes to your company's business continuity plan in the last five years?**





# FACT:

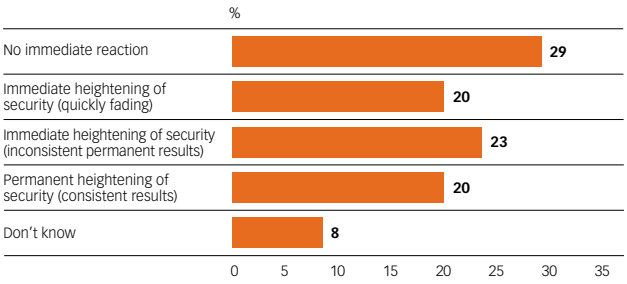
## ONE YEAR AFTER 7/7, MORE THAN HALF OF LONDON BUSINESSES HAD NO CONTINUITY PLAN IN PLACE

London Chamber of Commerce, 2006

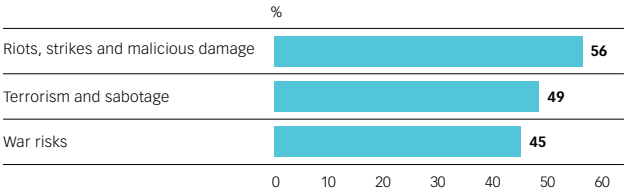
The research also reveals that only around half of companies are insured for political violence in emerging markets. Of those which are insured, many businesses believe they are covered under other policies, which may not be adequate, and a substantial minority of business leaders, more than one in ten overall, admit they do not know if they are covered or not. Demand for terrorism insurance is often lender-driven, and banks are unlikely to highlight the need for other cover such as war on land or riots and civil commotion, while companies operating in a range of territories across the world are likely to require different cover according to the region. Smaller companies are even less likely to have coverage in place.

Taken together, these results seem to highlight confusion about political violence insurance products, and the coverage they require. It suggests a clear need for companies to work with risk consultants and insurance brokers to review both their insurance needs in different parts of the world, and the range of insurance products available and where to get them. Otherwise the outcome for the company could be far from satisfactory when disaster strikes and the company is not covered, as Roscose explains: "We want to insure for being in the wrong place at the wrong time, not to be told we can't get a settlement because this was a terrorist attack."

**How do you believe your company would react to a major terrorist action receiving wide publicity?**




**Does your company insure its property in emerging markets against the following risks?**

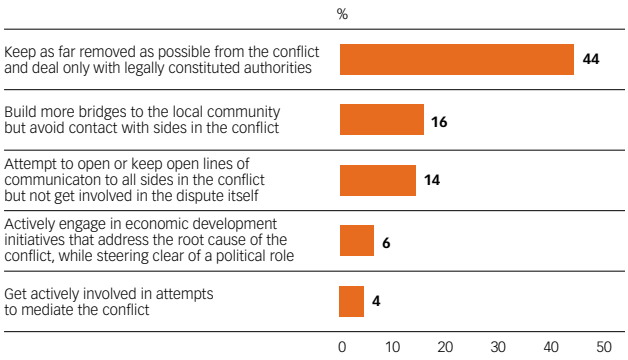


# "ONLY A SMALL MINORITY SAY THEY WOULD TRY TO BUILD BRIDGES WITH THE LOCAL COMMUNITY."

## FROM DEFENCE TO ACTIVE ENGAGEMENT

Companies in countries where the domestic political situation turns violent tend to take a defensive, low-profile position. Faced with such a situation, survey respondents most frequently answered that their company would "keep as far removed as possible from the conflict and deal only with legally constituted authorities" (44%). Only a small minority say they would try to build bridges with the local community or keep open communication with all sides in the conflict. By contrast, 32% say they would reduce or suspend operations in an overseas country experiencing political unrest, and 31% would put a greater emphasis on tighter facility security. Recalling the experience of conflict in Macedonia in 2001, Ms Sekerinska says that the business community tried to remain "invisible". Companies and business groups did not publicly endorse the negotiated settlement or even speak in favour of peace talks, despite all of them privately making clear their wish to see peace re-established.

**In the event of political unrest in an overseas country, which of these political strategies would your company be most likely to emphasise?**

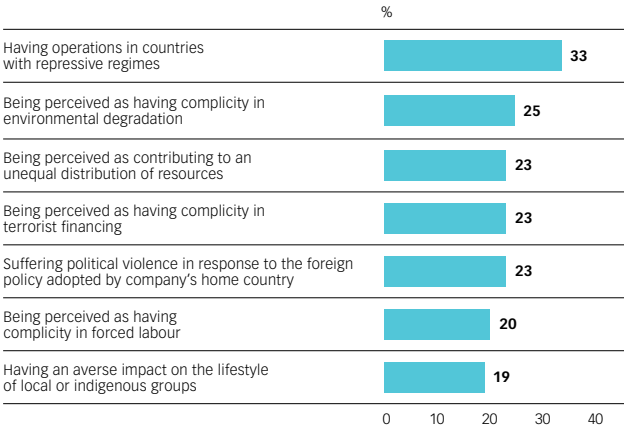



Unlike with international terrorism, some experts believe that laying low can be counter-productive when operating in countries undergoing intense domestic conflict. As noted earlier, companies are actors in the local situation whether they like it or not. Those involved in the struggle, as well as the broader international community, will be watching with increasing scrutiny. In such situations, corporate reputation is at stake.

Today, reputation represents an increasingly substantial proportion of a company's value but can take years to build, only to be damaged or destroyed in moments. A third of respondents believe that having operations in countries with repressive regimes or poor human rights records presents a moderate to major risk for their companies, and a quarter are concerned about contributing to unequal distribution of wealth in the territories in which they operate.

Reputation aside, Ms Sekerinska argues that executives need to address political issues as unrest grows to help restore stability. If they fail to do so, the resultant conflict becomes their problem. There are limits, however. Businesses are not embassies and excessive involvement in the political process could be dangerous or inappropriate. "There is very little that even a very large multinational corporation can do to address the root cause of problems. They are inherently political and governmental," says Mr Potter of Coca-Cola.

**Which of the following do you think present the greatest risks to your organisation?**



# THE STORY OF CELTEL:
## PROFITING FROM UNDERSTANDING POLITICAL RISK

Celtel, an Africa-based telecommunications company that was formerly known as MCI Cellular Investments, has grown from a US$11m start-up in 1998 to a company with US$1bn in annual revenue.

What sets Celtel apart from other successful telecoms companies is that it achieved this growth in 15 central African states, including some of the world's poorest nations and most violent trouble spots, such as the Democratic Republic of Congo, Sierra Leone, and now Sudan.

Dr Mo Ibrahim, Founder and Chairman, explains that the mainstream media generally paints Africa very negatively, focusing entirely on the problems, such as political violence and governance. In-depth, local knowledge gave Mr Ibrahim, who is African himself, a more nuanced view of the risks and opportunities in the continent's 53 states, rather than one fixating on the most troubled five or six countries. "Where perceived risk is higher than actual risk, it gives a window of opportunity," he reflects. This window was crucial to Celtel from the very beginning. "One aspect of being a risky country is that the big boys really shun you," he adds. Celtel could never have outbid the large industry players had they sought to bid for the mobile-phone licences in the countries where it started.

Operating in such environments is not always easy, or even possible. On the one hand, Celtel has on occasion had to tell staff to stay off the streets or evacuate them; once it turned over operation of a national network to a UN-sanctioned force which otherwise would have had a hard time communicating. On the other hand, the company has never experienced the politically motivated death of an employee or act of vandalism against its equipment. Mr Ibrahim explains that, providing his firm is perceived as neutral, all sides in a conflict can see the benefit of leaving the phone network alone. As with water, "people don't pollute wells when they know they will need them."

Neutrality does not, however, mean a lack of interest in the places where it operates. Celtel is heavily engaged in community relations and economic development projects, in addition to the substantial local economic activity brought about by its own operations. Such work is crucial in building up goodwill in the region. The company's African roots and personnel – half of top management and 98% of staff are from the continent – do not guarantee acceptance. "You can be African and a foreigner at the same time," says Mr Ibrahim. He points out that relationship-building with the local community is central to the company's mission and enhances the safety and security of his company's personnel and infrastructure when problems arise.

Accurate assessment of political risk, including the risk of violence, and engagement with the broader community in troubled areas are not just good practice. As the example of Celtel shows, they can also be sources of immense competitive advantage.

**"ACCURATE ASSESSMENT OF POLITICAL RISK... AND ENGAGEMENT WITH THE BROADER COMMUNITY... CAN ALSO BE SOURCES OF IMMENSE COMPETITIVE ADVANTAGE."**

# "THE KEY IS TO ALIGN ECONOMIC DEVELOPMENT INITIATIVES WITH CONFLICT RESOLUTION."

For international companies, something less active may be more appropriate. Mr Killick says: "We found early on that talking about peace put [business] people off. It was understood as being a political thing." However, companies can more easily see their role in economic development, which is where they can make the biggest difference.

The key is to align economic development initiatives with conflict resolution. This is sometimes referred to as "conflict-sensitive business practice," the absolute prerequisite for which is an in-depth knowledge of the conflict in question. Understanding these issues requires companies to build links with the community rather than hiding behind barbed-wire defences. Only through this kind of engagement and understanding can companies select the appropriate human rights, employment and environmental policies to bring general benefit.

More work and analysis to evaluate impacts, especially around human rights issues, would help to improve understanding in this area but the pay-off should not just eventually be a more peaceful and profitable environment. "Aligning human rights policies and community relations with the culture and values of the bank has a palliative effect in reducing exposure to political violence," says Mr Meyer. At ABB, according to Mr Roscoe, human rights, labour and environmental policies are integral to the company's security. "Links with the local community are critically important, especially in some Middle Eastern countries," he explains. "They can be the difference between an inefficient security system and spotting the problem. There is a tendency for companies to harden up security in certain territories, but it works better to link with communities, to explain that you are bringing something, so you can be seen as a force for good." Not engaging, howerver, is one of the biggest mistakes a firm can make because, in Mr Roscoe's words, "when you need help you'll be down the list". Physical barriers to keep trouble out, although sometimes necessary, can shut off companies from the local goodwill that is essential in a politically charged environment.

Of course, conflict-sensitive business practice is not easy to implement. "Undoubtedly, there are things that large companies, especially foreign direct investors, can do but defining best practice is at early stages," says Mr Potter. Fine judgements have to be made in efforts to be neutral and constructive. Ms Gardiner advises that balance is often the key, along with transparency and consultation.

The situation is evolving, with development and formalisation of standards a trend likely to grow. In the extractive sector, the Voluntary Principles on Security and Human Rights, originally an initiative of the UK and US governments, has led the way to new codes of conduct in other fields. Various toolkits have been produced, and continue to be adapted, to help companies assess challenging political situations and the impact on their businesses. The United Nations Global Compact put out a "Business Guide for Global Impact Assessment and Risk Management" in 2002 and, last December, the OECD and several other bodies jointly published "Business and Human Rights: the Role of Business in Weak Governance Zones." These important initiatives remain largely voluntary so far.

Mr Bickham notes that consultations surrounding codes such as the Voluntary Principles, and the codes themselves, help to ensure that companies remain aligned with rapidly changing expectations from society. For the major extractive companies, the involvement of their home governments in the process is also of value. So although there are no easy answers, best practice is now starting to be defined in this field, and increasingly it involves more than self-protection.

# CONCLUSIONS

## 1 THIS REPORT HIGHLIGHTS A RISING CONCERN AMONG BUSINESS LEADERS ABOUT THE RISK AND IMPACT OF POLITICAL VIOLENCE AS COMPANIES GLOBALISE.

While recent statistics indicate more stability than headlines suggest, the changing nature of war and terrorism means that business needs to have a comprehensive and flexible strategy to manage these risks.

## 2 TOO FEW COMPANIES DEVOTE THE NECESSARY RESOURCES TO RESEARCHING AND UNDERSTANDING THE RISKS.

Failure to make use of the multitude of information sources available on emerging threats can lead companies into a false sense of security. Equally, a flawed perception of risk will cause companies to miss investment opportunities in particular markets for the wrong reasons.

## 3 IT IS LIKEWISE CLEAR THAT COMPANIES NEED TO TAKE A MORE THOROUGH APPROACH TO PREPARATION AND RISK MITIGATION.

Unfortunately, a significant number are not even taking the basic steps – such as business continuity planning and formal co-ordination of risk management across the business. Of those who are, a substantial number now need to consider upgrading their plans and processes to address the growing issue of supply chain risk and give consideration to certain extreme events such as a nuclear, biological or chemical terrorist attack.

## 4 FOR COMPANIES OPERATING IN AREAS OF CONFLICT, HOWEVER, DEFENSIVE MEASURES ALONE ARE NO LONGER ENOUGH.

As the nature of local conflicts changes, and international expectations of business grow, companies will need to develop new risk management strategies. The good news is that a growing number of tools and standards of best practice are emerging to help companies.

## 5 IN PARTICULAR, BUSINESS LEADERS NEED TO CONSIDER PLAYING A MORE ACTIVE ROLE IN THE COMMUNITY AS PART OF A COMPANY'S SECURITY.

Business is a part of society: it benefits from peace. Tomorrow's successful companies will increasingly differentiate between when it is best to keep quiet in conflict and when it is best to make an effective, and potentially profitable, contribution to stability and reconciliation.

# FACT:

# "TERRORISM IS RELATIVELY CHEAP AND WILL BE WITH US FOR AS LONG AS ANYONE CAN ENVISION"

Walter Laqueur, Professor of International Security Studies, Washington DC


**Lloyd's** One Lime Street London EC3M 7HA Telephone +44 (0)20 7327 1000 Fax +44 (0)20 7626 2389 www.lloyds.com