



CCTV Plasa Kuningan (Samping sisi kanan Kec

360

TERRORISM IN ASIA WHAT DOES IT MEAN FOR BUSINESS?

THE GOVERNMENTS OF SOUTHEAST ASIA REMAIN ACUTELY AWARE OF THE POTENTIALLY DESTABILISING EFFECT OF ISLAMIST JIHADIST IDEOLOGY

Front cover image: In this CCTV frame grab handed out by police in Indonesia, a small truck, believed to be the suicide bombers', is seen shot from a building next to the Australian Embassy in Jakarta, seconds before it exploded at 10:30 am, on 9 September 2004.

TERRORISM IN ASIA

WHAT DOES IT MEAN FOR BUSINESS?

- 2** Executive summary
- 5** Understanding terrorism in Southeast Asia
- 12** What is the threat to business?
- 22** What can business do about the risk?
- 35** Conclusion

EXECUTIVE SUMMARY

For over 300 years, the Lloyd's insurance market has been helping business to prepare for and respond to uncertainty, and one of the greatest challenges currently facing global business is the threat of terrorism.

Lloyd's research has shown that although businesses are spending more time discussing terrorism at board level, many companies need to close the gap between increasing awareness of the risk of terrorism and a lack of understanding of what it means in practice.

Over the past year, Lloyd's has been working with the International Institute of Strategic Studies to evaluate the terrorism risk facing business and to assess what executives can do in response. This report focuses on Southeast Asia, a region of growing importance to the global economy and one not unfamiliar with the devastating impact of terrorism. We are most grateful for the support and the expertise of the IISS in providing an overview of the current terrorist threat in the region, and a series of practical recommendations on exactly how business leaders in Southeast Asia can better manage and mitigate the risks.

1 LIKE MOST REGIONS AROUND THE GLOBE SOUTHEAST ASIA IS NO STRANGER TO TERRORISM. HOWEVER, THERE IS NO SUCH THING AS A UNIFORM GLOBAL THREAT – THE REGIONAL THREAT IS UNIQUE AND COMPLEX AND OUR RESPONSE MUST RECOGNISE THAT

While the immediate threat from Islamist terrorism in the region appears to have reduced, terrorism has certainly not been eradicated. Communist insurgent groups remain active in the Philippines, regional insurgencies with varying degrees of Islamic influence are active in parts of Indonesia and Thailand, and politico-criminal gangs engaging in kidnapping and other forms of violent crime remain an active threat.

2 ANALYSIS OF INCIDENTS TO DATE IDENTIFIES A NUMBER OF COMMON THEMES WHICH CAN HELP COMPANIES TO MANAGE RISK

Some businesses and organisations are more vulnerable than others to terrorism in the region. In particular, a focus on certain targets using specific techniques means that the risk is likely to have a relatively predictable impact on the private sector, and with careful planning business should be able to manage and mitigate the risks with some success.

3 BUSINESS NEEDS TO GET BETTER AT GATHERING INFORMATION FROM THE RIGHT SOURCES AND USING IT TO GUIDE STRATEGY AND OPERATIONS

Local governments have done a great deal to help mitigate their local threats, and in addition most foreign governments provide assistance for companies investing in higher-risk locations – but business could gain more by better engagement. In addition, there is a wide range of expertise and advice available in the private and academic sectors which businesses should draw upon more effectively.

4 CORPORATE RESPONSE TO TERRORISM RISK ESSENTIALLY INVOLVES THE STRENGTHENING OF EXISTING RESILIENCE MECHANISMS, BUT NEEDS A POSITIVE MINDSET TOWARDS SECURITY

A corporate culture which sees security as a business enabler and not an hindrance, a well thought-out HR policy involving local employees, and effective business continuity planning all play an important role in protecting against terrorism.

5 IN THE LONG TERM, ERADICATION OF THE TERRORIST THREAT IS A GENERATIONAL CHALLENGE WHICH REQUIRES AN ACTIVE PARTNERSHIP ACROSS SOCIETY, AND THE PRIVATE SECTOR CAN PROVIDE AN IMPORTANT CONTRIBUTION

While the Al-Qaeda threat in the region appears to have diminished, it cannot be completely discounted, and the globalist Al-Qaeda ideology has undoubtedly taken a hold among sections of young Islamic populations around the globe. The private sector can do a lot to help with the engagement of communities whose young people are the most vulnerable to extremist ideology. Investment and HR decisions designed to help marginalised and economically disadvantaged communities, along with active engagement and a keen awareness of local traditions will not by themselves solve the problem, nor provide immunity from attack, but they all have an important part to play in creating a climate which is less receptive to the terrorist ideology.

TERRORISM IN SOUTHEAST ASIA ENCOMPASSES EVERYTHING FROM MILLENARIAN ANTI- WESTERN GROUPS TO LOCAL INSURGENCIES

PART 1

UNDERSTANDING TERRORISM IN SOUTHEAST ASIA

Over the past 20 years, there has been a noticeable shift in the world's centre of economic gravity towards Asia. Japan's emergence as an industrial and economic powerhouse in the 1970s was followed first by the rise of the "dragon economies" of South Korea, Taiwan, Singapore and Hong Kong, then by the "tiger economies" of Malaysia, Indonesia, Thailand and the Philippines. In the past decade, first China and more recently India have emerged not just as regional but global economic powers. Asia as a whole accounts for over 35% of global GDP – a figure that looks sure to rise. Asia's rise as a global powerhouse represents both an opportunity and a challenge for the international community. One such challenge is the threat posed by Islamist terrorism, a phenomenon present in varying degrees throughout the continent. The purpose of this report on Asia is to examine the nature of this threat specifically in Southeast Asia, with the aim of helping the private sector understand and evaluate the significance to them of this threat and to offer practical recommendations on how to mitigate it.

These broad statements summarise the nature of the threat in Southeast Asia and should serve to help those involved in managing risk better understand what they need to consider when assessing the threat to their operations in the region:

1 CURRENT LOWERED RISK

While international and regional terrorism have by no means been extinguished in the region, the decline in terrorist incidents in the region over the past three years would indicate that the threat has receded from an earlier peak in the late 1990s and early 2000s.

2 COMMUNIST TO ISLAMIST THREAT

The threat from post-Cold War socialist political groups has lessened, but Islamist insurgencies have filled the void, while communist influences remain obvious in certain regions.

3 AL-QAEDA CONNECTIONS FALTERING

It is too early to state that the connection to international terrorism has been severed in the region, but there has been a noticeable disengagement between local groups and Al-Qaeda.

4 LOCAL INSURGENCIES PREDOMINATE

The main threat to be considered in the region has shifted from international Islamist groups to specific regional issues driving insurgencies.

5 TERROR AND CRIMINAL NEXUS REMAIN

Nevertheless, some element of risk remains for business investing in the region: kidnapping for ransom remains a favoured fundraising tool and groups have bombed major industrial sites, tourist locations, and transport routes, as well as religious sites like Christian churches or Buddhist temples.

BACKGROUND

Southeast Asia has been no stranger to terrorism and politically-motivated violence over the course of its modern history. Much of this violence had its origins in the struggle for independence from Western colonial government and drew on Marxism-Leninism for its inspiration, a trend that continued into the latter half of the 20th century as a by-product of the Cold War. But a combination of the collapse of the Soviet Union, China's gradual move towards a market economy and a sustained period of economic growth and modernisation throughout Southeast Asia meant that by the 1990s communism had largely lost its appeal. Only in the Philippines did the communist New People's Army (NPA) continue to pose a significant security threat.

But as the threat posed by communist groups receded, Southeast Asia saw the emergence of a new security threat from extremist Islam. This phenomenon was fuelled by the efforts of Saudi Arabia to promote its austere fundamentalist Wahabbi version of Islam to counter the Shia ideology exported by Iran after the overthrow of the Shah, and by the Soviet invasion of Afghanistan. In particular the war in Afghanistan acted as a rallying point for young Muslims from around the world, many of whom - including some from Southeast Asia - made their way there to take part in jihad or holy war against the Soviet invaders. Afghanistan was a defining experience for many of these individuals who subsequently returned to their own countries radicalised by their experiences and imbued with a desire to impose a "pure" version of Islam through violent action. Many of these returnees became affiliated to Osama bin Laden's global Al-Qaeda organisation.

Southeast Asia's vibrant economic growth, good communication links and more relaxed visa regimes made it an attractive operating base for some of the individuals who subsequently became part of Al-Qaeda. These individuals established a regional network based in the Philippines, funded by Osama bin Laden's brother-in-law and headed by Ramzi Yousef, the architect of the 1993 bombing of the World Trade Centre. In 1995, this network was broken up after the discovery of plots to assassinate Pope John Paul II and Bill Clinton on visits to Manila, explode bombs on almost a dozen airliners flying from Southeast Asia to the USA (Operation Bojinka) and to fly a light aircraft into CIA headquarters. Nevertheless, the region continued to be used as a facilitation base by Al-Qaeda and several of the operatives involved in 9/11 passed through Kuala Lumpur en route for the USA.

SOUTHEAST ASIA SAW THE EMERGENCE OF A **NEW SECURITY THREAT** FROM EXTREMIST ISLAM



JEMAAH ISLAMIAH AND INTERNATIONAL TERRORISM IN SOUTHEAST ASIA

The end of the 1990s saw the emergence of an indigenous Southeast Asian terrorist organisation, Jemaah Islamiah (JI), which was founded by two Indonesian clerics exiled to Malaysia, Abdullah Sungkar and Abu Bakar Bashir, with the aim of creating a Caliphate uniting all the states of Southeast Asia. Following the collapse of the Suharto regime in 1999, Sungkar and Bashir returned to Indonesia where they established a network of religious schools or pesantren to promote the JI ideology. At the same time, Abu Bakar Bashir set up a political front organisation, the Majelis Mujahidin Indonesia, a development that reflects a continuing dichotomy of views within JI about the use of violence to achieve their aims, with some tending to the view that violence would be counter-productive. But from 2000 to 2005, JI was responsible for a series of terrorist attacks including the 2002 and 2005 Bali bombings and the bombings of the JW Marriott Hotel and the Australian Embassy in Jakarta in 2003 and 2004 respectively. During that period, JI also had strong links to Al-Qaeda, notably through its head of operations Riduan Isamuddin, otherwise known as Hambali, who had known Osama bin Laden in Afghanistan.

Although JI's most spectacular terrorist operations took place in Indonesia, it had a network of cells and supporters throughout the Southeast Asian region. JI was able to benefit from the existence of numerous terrorist training camps in Mindanao in the Philippines run by separatist and politico-criminal groups like Abu Sayyaf, the Moro Liberation Front (MLF), and the Moro National Liberation Front (MNLF). As well as bolstering JI, both the Moro liberation organisations and Abu Sayyaf have independently been responsible for a further string of terrorist incidents in the Philippines including bomb attacks in urban centres, on ferries and other transport links, and regular kidnappings.

Beyond the Philippines, JI's influence has reached into Singapore, where a JI cell was arrested at the end of 2001 when it became clear that the group was planning to attack Western diplomatic missions using truck bombs. More recently, in January 2008 the Singaporean authorities arrested a group of activists planning to undertake a jihad overseas. While Malaysia and Thailand have experienced no JI-related attacks, there has been evidence of JI activity in both nations. Across the border from Thailand in Cambodia, the minority Cham population, almost annihilated under the Khmer Rouge, has been targeted for recruitment by radical Islamic organisations like Tablighi Jemaat.

For Thailand, however, a more immediate terrorist threat emanates from a resurgence in 2004 of a long-running, but previously low-key, separatist insurgency by the ethnically Malay Muslim minority in the country's four southernmost provinces. So far there has been no evidence of any attempt either by JI or Al-Qaeda to become involved in this conflict, but it has still produced in excess of 2,400 deaths over the past three years.

THE CURRENT SITUATION AND THE RESPONSE OF REGIONAL GOVERNMENTS

The emergence of a significant Islamist terrorist threat presented the governments of Southeast Asia with a complex challenge: how to preserve their reputation as safe destinations for investment and tourism while avoiding alienating Muslim populations who constitute either the majority or a politically sensitive minority.

INDONESIA

This dilemma is particularly acute for the Indonesian government when it contemplates how politically to justify proscribing an organisation, Jemaah Islamiah, whose name means "Islamic Society". Nevertheless, following the 2002 Bali bombings, the Indonesian authorities arrested and tried both the bombers themselves and their "spiritual leader," Abu Bakar Bashir, who served a short prison sentence. The elite and Western-trained Indonesian police unit Detachment 88, which had undertaken the Bali investigation with the assistance of the Australian Federal Police, went on to achieve significant success in arresting the leadership of JI's terrorist wing. Consequently there have been no serious terrorist incidents in Indonesia for over two years. However, the consensus among expert opinion is that JI has in effect declared a unilateral truce rather than having abandoned violence and that debate continues within the movement about the utility of violence. If JI does decide to resume violence, evidence gathered in police raids of JI hideouts in the summer of 2007 suggests that this may be focused primarily against indigenous Indonesian targets rather than foreign institutions.

SINGAPORE AND MALAYSIA

Both the Singaporean and Malaysian authorities have made strenuous efforts to engage the support of their Islamic populations against extremism and have devoted significant resources to developing counter-radicalisation and de-radicalisation programmes. The former aimed at preventing new terrorists from emerging and the latter at winning back those who have succumbed to extremism. The degree to which these programmes have been successful is hard to determine, but to date both countries have managed to avoid suffering major terrorist attacks.

PHILIPPINES

In the Philippines, the armed forces have been conducting a sustained counter-insurgency campaign in Mindanao and the Sulu archipelago with significant US support, while simultaneously pursuing peace negotiations brokered by the Malaysian government. These talks have resulted in the delineation of an autonomous Moro region within Mindanao, which should in principle meet the key demands of the main separatist insurgent groups. It is, however, unlikely that the Abu Sayyaf group – now arguably less a terrorist group than a profit-driven criminal organisation - will cease operations as a result of this agreement. A tradition of lawlessness combined with complex local politics makes it likely that Mindanao will remain a source of regional instability for some time to come.

THAILAND

The response of the Thai authorities towards the insurgent movement in the south has been characterised by an inconsistent approach involving competition between the police and the Royal Thai Army and the use of a combination of carrot and stick. Latterly the Thai authorities have begun to make progress both in collecting intelligence and winning the support of segments of the minority Muslim population. There is, nonetheless, no sign of a readiness to seek a negotiated solution to this problem even if the insurgent groups involved were prepared to engage in talks, which they have so far shown no readiness to do.

CONCLUSION

Based on an objective evaluation of the facts on the ground and discussion with official and non-official experts, there can be no doubt that the overall situation in respect of Islamist terrorism in Southeast Asia is better than it was at the start of the millennium.

The governments of the region have in the main recognised the potential severity of the threat and have begun to take steps at both national and regional level to combat it. Although initially JI had close links with Al-Qaeda, latterly there has been no evidence of any continuing communication or relationship between the two organisations and for the most part, the biggest threat in the region is from local terrorist groups with regional agendas. In Indonesia, the world's most populous Islamic state, there have been no significant terrorist incidents for over two years and moderate Islamic groups have begun to dominate the political discourse.

Nonetheless, the governments of Southeast Asia remain acutely aware of the potentially destabilising effect of Islamist jihadist ideology and are maintaining a high level of vigilance against the possibility of a resurgence of terrorist activity.

**GOVERNMENTS OF THE
REGION HAVE IN THE
MAIN RECOGNISED THE
POTENTIAL SEVERITY OF
THE THREAT AND HAVE
BEGUN TO TAKE STEPS
AT BOTH NATIONAL AND
REGIONAL LEVEL TO
COMBAT IT**

PART 2

WHAT IS THE THREAT TO BUSINESS IN SOUTHEAST ASIA?

The threat from terrorism in Southeast Asia encompasses everything from millenarian anti-Western groups to local insurgencies with varying shades of Islamist tendencies. This general threat assessment is reflected in the types of attacks that business in the region needs to be aware of and mitigate against – covering everything from “traditional” terrorist attacks on what are seen as Western targets, to politico-criminal gangs with profit motives, to insurgencies seeking to undermine a central government. Every business in Southeast Asia will have a different presence and consequently certain aspects of the below list will affect them in different ways and in different places. The list reflects a series of running themes among local terrorist plots and actions that those who manage risk should consider:

1 “WESTERN” TARGETS

This concept must be taken in its broadest possible sense. In many of the plots detailed in this section, targets have been selected solely on the basis of their Western links.

2 PROXIMITY TO EMBASSIES OR HIGH COMMISSIONS

Often the most visible expression of foreign presence in a city, embassies have been targeted repeatedly. As they tend to be located in prime real estate in the centres of cities, many other businesses, either local or foreign, located nearby tend to suffer collateral damage from any attack.

3 VISITING DIGNITARIES

Visiting dignitaries have been targeted for attack. Fortunately no attacks have succeeded so far, it is likely that in the event of an attack the surrounding location would suffer casualties and damage.

4 HOLIDAY RESORTS

These are an obvious target, especially those in remote locations.

5 TRANSPORTATION ROUTES

Plots listed in this section show that local groups have targeted aviation, shipping, and land-based transportation.

6 KIDNAPPING

There are some remote and less developed parts of Southeast Asia where government control is at best partial. For example, Southern Thailand and the Sulu Islands in the Philippines are known Islamist and insurgent hide-outs where foreigners are advised not to travel, and even locals should be careful.

7 POTENTIAL UNDERLYING CRIMINAL MOTIVE

The line between terrorist/criminal/insurgent is often blurred in Southeast Asia. For business managers, this means that the threat of being targeted by one of these groups for ransom or extortion cannot be discounted, a reality that must be borne in mind when trying to evaluate the local terrorist risk.

8 POLITICAL INSTABILITY AND SMALL INSURGENCIES

Specific regions in Southeast Asia (southern regions of Thailand; Mindanao region of the Philippines and Sulawesi and West Papua regions of Indonesia) face low-level separatist or other insurgencies and should be approached with particular care.

BALI BOMBINGS

12 OCTOBER 2002 AND 1 OCTOBER 2005

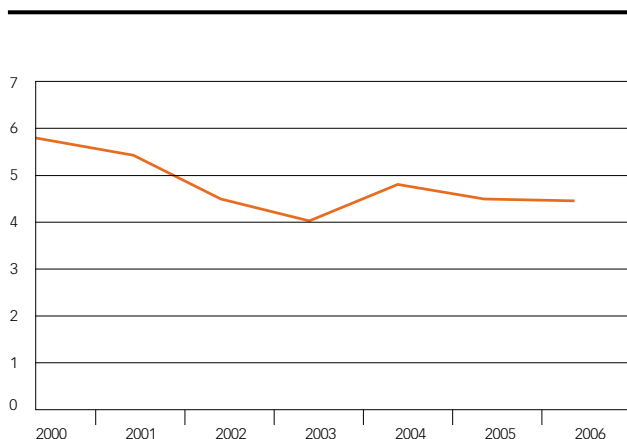
On 12 October 2002, three bombs were detonated in the Indonesian resort of Kuta, Bali, causing the deaths of 202 people, of whom the majority were foreign tourists (among the dead were 88 Australians, and 64 Indonesians). Three years later, on 1 October 2005, bombers struck again in Kuta, and also in nearby Jimbaran. Most of the 20 people who were killed in this second wave were Indonesian, but Australians and Japanese (the two biggest single tourist groups to visit Bali) also died.

The casualties of the second wave could have been much higher if the three further devices found that had failed to explode had been detonated.

Impact on business:

Aside from the human cost, Indonesian tourism suffered dramatically in the wake of both attacks, with numbers dropping noticeably in the immediate period following each attack. 9/11 had already caused a pronounced drop in international flights and a consequent drop in tourism, and the continued attacks in Indonesia have had a noticeable impact upon tourist revenue figures.

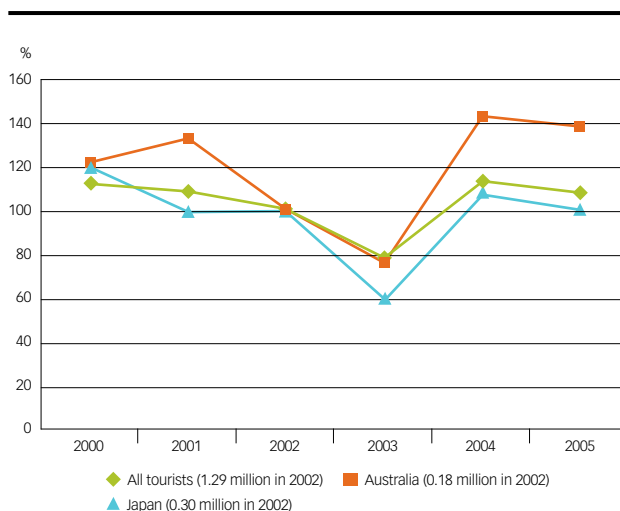
Revenue from tourism (US\$Bn)



Source: Statistical Report on Visitor Arrivals to Indonesia

For Bali, the impact was especially high, with noticeable drops in Japanese and Australian tourist numbers in particular. While the figures for 2006 and 2007 show noticeable improvements, the local economy has yet to completely recover, with one report indicating that there have been 22 restaurant and hotel closures in a hilltop resort in Bali since the 2002 attack.

Percentage of tourists to Bali relative to 2002 levels



Source: Bali Tourism Board

This was exactly the effect the bombers were seeking. Following the attack, Imam Samudra, one of the organisers of the plot, was quoted as saying that he had been disgusted by “the dirty adulterous behaviour of the whites there”. As well as citing American actions (with Australian support) in Iraq and Afghanistan as their motivations, they also saw the nightclubs and bars of Bali as a part of a cultural assault on the Islamic world (though it is worth highlighting the fact that Hindu is the majority population in Bali). The enemy, according to Ali Ghufron, one of the other plotters, also known as Mukhlis, was “capitalist terrorists” whose “programmes of destruction and lust” undermine Islam.

JAKARTA MARRIOT BOMBING 5 AUGUST 2003 AND AUSTRALIAN EMBASSY BOMBING 9 SEPTEMBER 2004

On 5 August 2003, a suicide bomber detonated a car bomb outside the JW Marriot Hotel in Jakarta killing himself and 11 others, as well as injuring many more. Almost a year later, on 9 September 2004 another suicide bomber, this time in a van, blew himself up outside the Australian Embassy in Jakarta killing between nine and 11 people and injuring scores of others. In both attacks, the vast majority of the victims were Indonesian, with one Dutch businessman reported dead in the first blast.

Both attacks (and the earlier Bali bombings) were subsequently claimed or attributed to Jemaah Islamiah (JI), a local terrorist group some of whose members have been reported as having links to Al-Qaeda in the past. The bomb makers in both cases were revealed to be the same, and trace elements of chemicals from both bombings were connected to other attacks. While many of the support networks have been dismantled and key players arrested, a number of key suspects, including mastermind Noordin Mohammed Top, remain at large.

Impact on business:

The most obvious direct impact to business in the case of these two attacks, aside from the human cost, was the damage done to the target buildings and their immediate vicinities. The JW Marriot hotel absorbed the main impact of the first blast and remained closed for five weeks, finally re-opening on 8 September 2003. The owners estimated that repairs and lost custom cost the hotel \$8m. A nearby shopping mall, the Plaza Mutiara, also absorbed a substantial amount of the blast, though neither building suffered major structural damage.

The 2004 attempt on the Australian Embassy had much the same effect, although the bombers inability to get close to the Embassy compound, thanks to the fact it was set back from the road and behind a metal fence, meant that nearby office blocks ended up suffering more.

Both attacks caused a drop in the Indonesian stock market: the Marriot blast 3.1% and the Australian Embassy blast 4%. In both cases, however, markets proved resilient and bounced back swiftly. Looking back at the previous section on Bali's charts, this seems at least partly attributable to the prevailing downward trend in tourism revenue in Indonesia to the terrorist strikes. One specific figure cited in respect of this was in the wake of the Australian Embassy bombing, when

hotel occupancy dropped by half, although by March of the subsequent year it had recovered by about 70%.

One fact to be drawn from these and other attacks in Indonesia (the Bali bombings and attacks or attempts by JI in 2000 and 2001) was the tendency for attacks targeted at Western or Christian targets to take place towards the end of the year. This has resulted in higher levels of security in subsequent years, though fortunately an attack has not materialised.

While the bombers targets were overtly Western symbols (the JW Marriot was known to be popular with Western tourists, and had hosted the American July 4th celebrations for the previous two years), most of the damage was absorbed by the surrounding buildings and population.

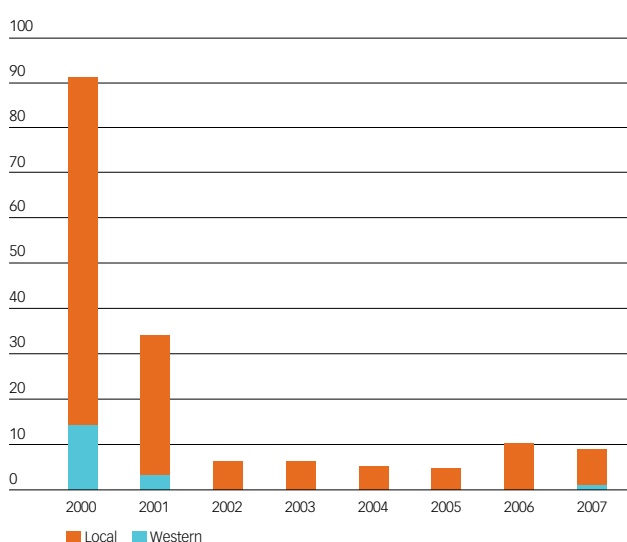
Subsequent investigation also uncovered the fact that, at least in the case of the Marriot attack, the hotel had not been the only target taken into consideration. Other potential targets included a Citibank branch, the Australian International School and the Jakarta International School.

KIDNAPPING AND THE ABU SAYYAF GROUP (ASG) IN THE PHILIPPINES

Established in the early 1990's by a Filipino, Abdurajik Janjalani, who had fought with Osama bin Laden in Afghanistan, the Abu Sayyaf Group (ASG) (named after Janjalani's nom de guerre Abu Sayyaf) is a predominantly Philippine extremist group drawn from elements of a local separatist group the Moro National Liberation Front (MNLF). One of the ASG's most notorious tactics is kidnapping for ransom, with a preference for targeting Westerners.

It is worth highlighting that the overwhelming majority of Abu Sayyaf's kidnap victims are local, with figures drawn from the IISS Armed Conflict Database suggesting that less than 10% were Western. At least 147 Philippine nationals have been kidnapped by the group since 2000, and many more have been killed in other actions in a campaign that has been going on since 1991. It is also necessary to highlight the deep unreliability of specific kidnap figures as families or individuals may have chosen to pay a ransom and not report the kidnap. Nonetheless, the broad trends pointed to in this section remain accurate.

ASG victims by provenance



Source: IISS Armed Conflict Database

Impact on business:

The most obvious threat to business comes from the danger to personnel who have to travel, either for business or pleasure, in regions where ASG are active. If the individuals are there on company business, then it immediately becomes an issue for the employer who might be expected to help meet any ransom demand. On top of this, if the region is of particular interest to a company or industry, the added costs of personnel security may diminish the attraction of investment in the region. The fact that international aid projects and tourists have been the subject of attacks suggests that any major corporation which sets up operations in the area would be equally vulnerable. Further afield, ASG have targeted Malaysian tourist resorts like Sipadan, a remote island popular with scuba divers, though their main base of operations would appear to be the Jolo Island in the Sulu Archipelago.

The purpose of kidnapping Westerners appears not to be to make a political or propaganda point, as has been the case in the Middle East, but rather to extort ransoms. Abu Sayyaf has also carried out mass executions of local residents seen as unbelievers (typically local Christians) or government agents. Foreigners are far more likely to be held to ransom (though American hostages have been executed for reasons which remain unclear). The bigger threat to captured individuals would often appear to be during attempted rescues, when they have been caught in the cross-fire. While more recently governments have started to refuse to pay ransoms, this has not always been the case, providing an incentive for such activities to continue. For business in the region this presents a further potential expense, beyond the human one, should staff become embroiled in such a kidnapping.

MARITIME THREATS IN THE REGION

On 27 February 2004, a suicide bomber detonated himself on SuperFerry 14, a civilian carrier ship from Manila, sinking the ship and killing some 116 passengers. This incident has gone down in history as the most lethal instance of sea-borne terrorism. But such episodes have been rare, with the main maritime threat in Southeast Asia coming from piracy.

In the subsequent investigation into the SuperFerry 14 incident, the government claimed that the ship had not been chosen at random; apparently Abu Sayyaf had targeted the company for retribution since they had refused to pay protection money.

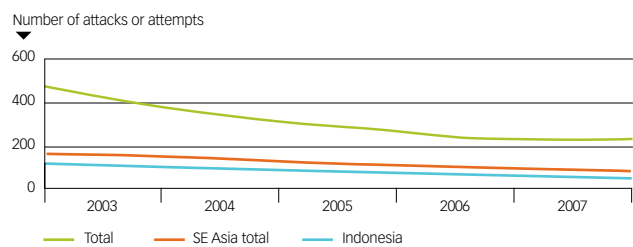
Impact on business:

The threat from a SuperFerry 14 type attack is something that is hard for companies to ever completely insulate themselves from, and consequently calculating the impact upon business remains almost impossible. Often, however, the greater concern from a business perspective in the region is piracy rather than terrorism. While this threat is often inflated (though admittedly accurate information is not always easy to obtain) it certainly remains the more likely risk that risk managers need to mitigate.

Broadly speaking, the trends in the region are positive, with the International Maritime Bureau (IMB) reporting that actual and attempted attacks are in decline. This reflects a broader trend internationally, and these figures must be set in the context of the many thousands of ships that sail the seas unimpeded by terrorists or pirates.

Furthermore, in volume terms as a proportion of global instances of maritime piracy, the specific threat in Southeast Asia is further in decline, reflecting a greater vigilance by shipping in the region and increased efforts by local governments.

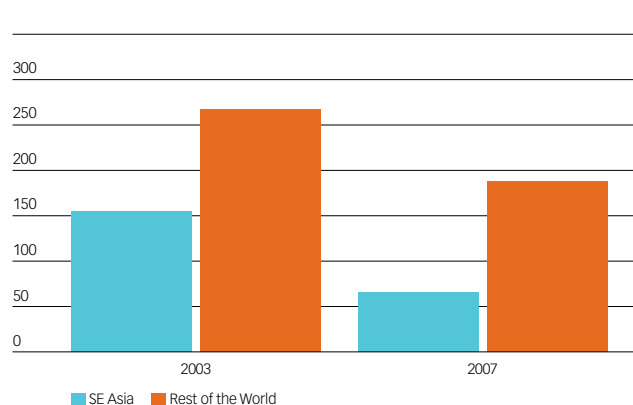
Piracy in SE Asia



Source: ICC International Maritime Bureau Annual Report, January 2008

This is particularly the case in the Malacca Straits where governments have been especially successful in tackling piracy and ensuring the safe passage of the more than 50,000 vessels and roughly 15 million bbl/d of oil (2006 figures) that transit through the Straits every year.

Instances of Piracy Globally



Source: ICC International Maritime Bureau Annual Report, January 2008

POLITICAL INSTABILITY AND SMALL INSURGENCIES

Beyond traditional terrorist groups with internationalist aims or criminal intentions, nations in the region face localised insurgencies and specific areas, broadly speaking, remain out-of-bounds to investors. Driven by a variety of political motivations, from neo-communist to Islamist, but for the most part motivated by traditional separatist aims, these groups pose a risk to any outsider who enters their terrain. As Prime Minister Abdullah Ahmad Badawi of Malaysia has pointed out, “terrorism [in the region] is essentially driven by domestic factors and has a domestic agenda.”

The line between more traditional separatist groups and other transnational terrorist groups is hard to definitely draw, and connections between terrorist groups like Jemaah Islamiah or Abu Sayyaf and separatist groups (specifically those pursuing separatist aims of the Moro peoples) have been charted.

Impact on business:

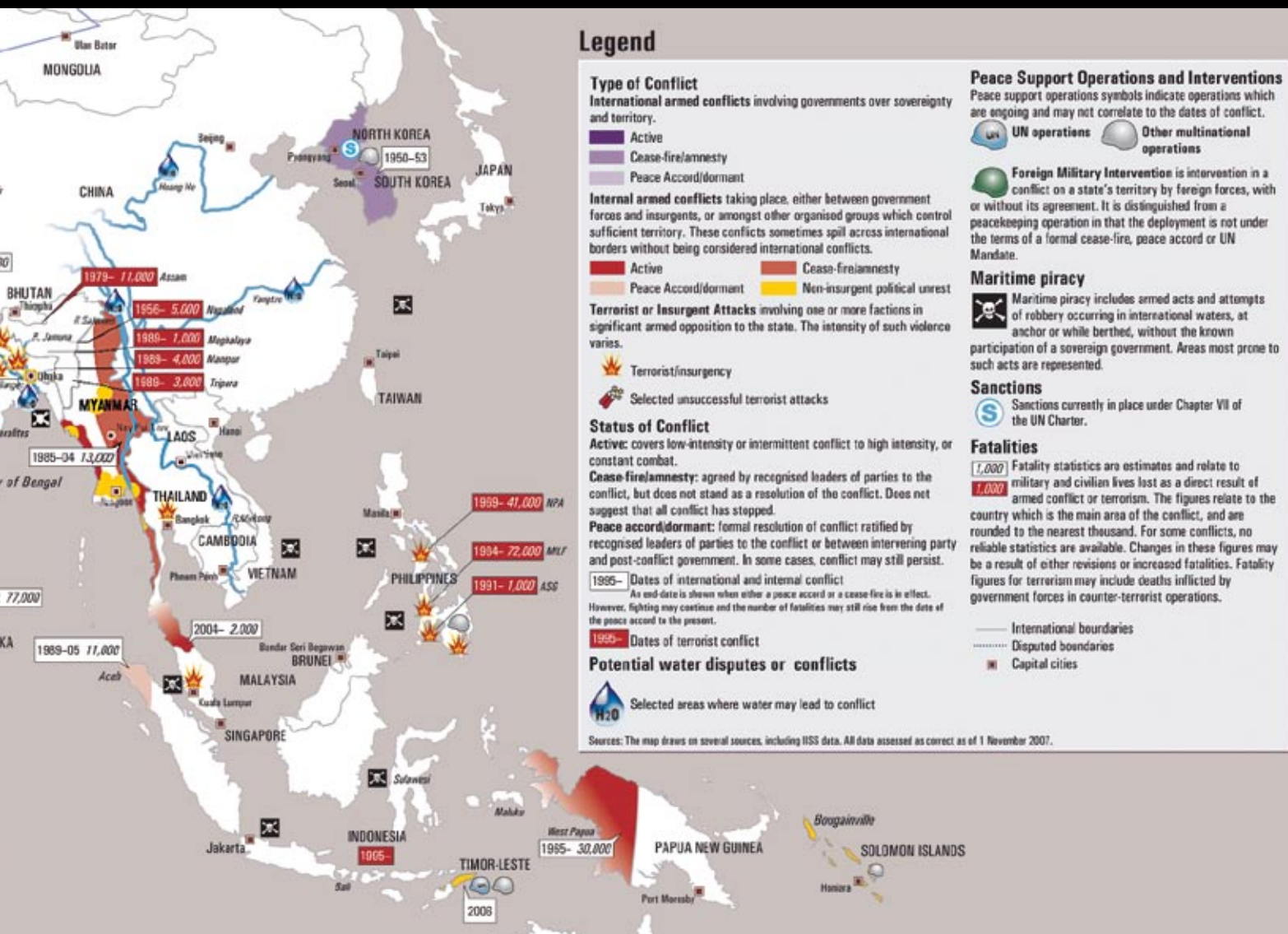
These insurgencies create instability and make regions unwelcoming to outside investment: for business these areas would likely be considered no-go. For the most part, these areas lie outside government control, so any attempt to seek local assistance or recourse is likely to be met with failure. For businesses that remain eager to invest in these regions, it is best to seek both local governmental support, but also assistance from professional international firms that specialise in security in the region.

A complete list of the many terrorist and insurgent groups currently active in this region can be found in Appendix 1, but generally speaking the following regions should be approached with care:

- Southern Thailand
- Mindanao region of the Philippines
- Sulawesi and West Papua regions of Indonesia.

This is not to say that they are comprehensively no-go areas, but attention should be paid, especially when seeking to invest in the regions, that precautions have been taken and the potential risk has been taken into account.

**THE BIGGEST THREAT
IN THE REGION IS FROM
LOCAL TERRORIST
GROUPS WITH
REGIONAL AGENDAS**



UNCOMPLETED OR FOILED PLOTS

“Bojinka” Plot

On 11 December 1994 an explosion on Philippines Airlines Flight 434 between Manila and Tokyo killed passenger Haruki Ikegami, a Japanese national. The damaged aircraft managed an emergency landing in Okinawa and only ten other passengers and staff of 272 on the Boeing 747-200 were injured.

The origin and explanation for this seemingly random and minor attack were only made clear weeks later, in the early hours of the morning of 7 January 1995 at a fire in an apartment in Manila. Police arrested one individual, Ahmed Saaed, and in the subsequent investigation of the materials found in the apartment and interviews with plotters both at the time and years later the parameters of the plotters ambitions were laid out as thus:

- Bomb as many as 12 airliners originating and in transit between American and Asian airports (including Hong Kong, Manila, Taipei, Tokyo, Singapore, Seoul) using devices ten times as strong as those used on Flight 434
- Crash an aircraft into the Central Intelligence Agency (CIA) headquarters in Langley, Virginia
- Attack Pope John Paul II and Bill Clinton’s motorcades with explosives, suicide bombers or stinger missiles while they were visiting Manila.

Had the plot succeeded, the damage done may have eclipsed the 9/11 attacks, and elements of these plans may have been reflected in a number of subsequent Islamist terrorist attacks and plots. The mastermind, Ramzi Youssef, was also responsible for the first attack in 1993 on the World Trade Center in New York and he was finally captured in Pakistan in February 1995.

2001 Singapore Embassies Plot

In December 2001, Singaporean security services swept in and arrested 13 members of a Jemaah Islamiah sleeper cell that had targeted a broad array of local targets. Recently activated by the arrival of two external members, the group was made up of native Singaporeans, who for the most part had remained below the radar of local intelligence services.

Soon after the arrests, American forces in Afghanistan uncovered a videotape in the bombed-out house of a senior Al-Qaeda member that showed a series of Singaporean targets and appeared to offer some ideas of how they could be struck. While it is unclear whether the group was initially given funding by Al-Qaeda to pursue its actions in Singapore, around the time of the 9/11 attacks the decision was made to activate the group. Since the cell was arrested before they could go beyond reconnoitring their intended targets and source explosives, the list of potential targets is speculative – although based on intelligence from security services. It emphasises broader trends in regional terrorism, and specifically in targets pursued by Jemaah Islamiah elsewhere.

Potential targets:

- American, Australian, British and Israeli embassies in Singapore (and possibly beyond in the Philippines, Indonesia and Malaysia)
- The Yishun Mass Rapid Transit (MRT) Station
- A local shuttle transport bus utilised by American Embassy staff
- Prominent American businesses in Singapore, and commercial buildings in which they were housed
- The Singaporean Ministry of Defence complex at Bukit Gombak
- A US naval vessel in the waters off Singapore between Changi and Palau Tekong
- A member of the group had worked as a technician at Paya Lebar Airbase, which is used by US Air Force, and was instructed by other cell members to take pictures of the aircraft at the base.

PART 3

WHAT CAN BUSINESS DO ABOUT THE RISK?

Building resilience against terrorism is an extension of resilience to other more traditional threats, and most businesses should already have plans in place to protect against contingencies such as fire, theft, kidnapping and fraud wherever they are based in the world. Strengthening these defences is the best way to counter terrorist threats. This final section presents ideas which, both over the short and long term, can help business mitigate the risk it faces. It also includes suggestions as to where business can go for help, and on the role that it can play in supporting local governments:

1 AS IS BROADLY THE CASE INTERNATIONALLY, THERE IS CURRENTLY A RELATIVELY LOW PROBABILITY OF A DIRECT TERRORIST STRIKE AGAINST BUSINESS INTERESTS OR FACILITIES IN SOUTHEAST ASIA, BUT THE RISK OF INDIRECT DAMAGE IS OFTEN OVERLOOKED

As this report has shown, instances of international terrorism in Southeast Asia are relatively low, and may be decreasing. However, they cannot be totally discounted, and those who manage risk should have some awareness of their proximity to possible targets and international investors might be seen as a target because of their nation of provenance.

2 BETTER INFORMATION GATHERING

Terrorism in Southeast Asia is by no means static, either in terms of tactics or aims. There are many individuals and groups in both government and the private sector who have considerable knowledge and expertise about specific regions and groups. Finding out who these individuals and firms are and understanding where available information can be sought is a crucial start for businesses seeking to understand and manage the threat to investments in this region.

3 POSITIVE AND HOLISTIC MINDSET

Organisations should adopt security as part of the corporate culture and regard good security practice as a business enabler, not a hindrance. Organisations should consider terrorism early on in planning stages of organisational moves or in the design of a new building, as well as in the construction of any computer systems. Companies should make sure they have taken obvious precautions to mitigate the direct threats to the organisation and ensure that business continuity plans are tested and updated regularly. Furthermore, ensuring good emergency lines of communication with employees will increase staff confidence in the company. Finally, while the threat from a cyber attack is limited, the possibility cannot be completely discounted.

4 UNDERSTAND AND PROTECT YOUR SUPPLY CHAINS

A major aim of terrorist groups is to inflict large-scale and random economic damage. Understanding exactly what your supply chain looks like locally is critical in ensuring that you have sufficiently mitigated the risk to your business.

5 ENGAGE WITH THE WIDER BUSINESS COMMUNITY, GOVERNMENT AND SOCIETY ON THE ISSUE OF TERRORISM AND SECURITY

Ultimately, no amount of proactive or preventive measures can offer full protection against terrorist attack. However, greater engagement on this issue with all the stakeholders, at home and abroad, will help society mitigate this problem. Smart and sensitive human resources policies and developing a strategy to engage and employ local communities as part of a comprehensive CSR policy are all long-term steps that business can take.

1. As with the terrorist threat internationally, currently the first thing for any business in Southeast Asia to note is the relatively low probability of a direct terrorist strike against its interests or facilities.

More likely is that a business will find itself physically located near an intended target and suffer disruption to its operations as a consequence. Even if a business does not suffer direct physical damage, it may find that its staff is unable to get to work in the wake of an event, or that a link in its supply chain has been either directly or indirectly hit. Beyond this, certain industries, such as retail or tourism, may find themselves affected by a terrorist strike with a sudden drop-off in sales in the immediate wake of an attack.

However, there are more specific risks that must be borne in mind by risk managers for certain businesses operating in different parts of the region. Companies that are perceived as Western, for example, are likely to face a more elevated threat from Islamist terrorists. As Singaporean Minister Mentor Lee Kuan Yew put it when describing an attempt on his nation, “they [the plotters] had nothing against Singapore. Their target was the US.” While this report seeks to offer a broad overview of the possible threats, they are constantly evolving, and those who manage risk should update themselves regularly about the specific part of the world they are operating in.

2. Better information-gathering.

Make full use of the sources available to get the right information and advice and work in partnership with these sources to identify the gaps for your business. There is a considerable amount of information already available to help business think through some of the contingencies associated with terrorism and security in Southeast Asia, some of which is laid out here.

WHERE CAN YOU GO FOR HELP?

There are various government agencies working to help face the threat of terrorism. The following list sets out who provides what advice and how to contact them:

First points of contact:

In the event of a terrorist or any other incident, your first point of contact should be **the local police and your local embassy or high commission**. Below is a list of the first points of contact in the respective nations covered in this report:

- **Indonesia**
Police website: www.polri.go.id
- **Malaysia**
Police website: www.rmp.gov.my
- **Philippines**
Police website: www.pnp.gov.ph
- **Singapore**
Police website: www.spf.gov.sg
- **Thailand**
Police website: www.royalthaipolice.go.th

The following is a list of key Southeast Asian government ministries and agencies dealing with terrorism:

Singapore: Counter-terrorism is primarily the responsibility of the Interior Ministry. The Internal Security Division of the Ministry is in effect the Singaporean security service. It is well resourced and highly regarded.

Malaysia: The Royal Malaysian Police Special Branch has primary responsibility within Malaysia for combating terrorism. It is large, well resourced and highly regarded. Malaysia is also home to the Southeast Asia Regional Centre for Counter Terrorism (SEARCCT), a US supported training centre that specialises in counter-terrorism training for the region.

Indonesia: Indonesia has a civilian intelligence and security service (BIN) and a military intelligence service (BAIS) both of which are engaged in counter-terrorist work. However, primary responsibility for counter-terrorism investigations lies with the Indonesian police (POLRI), and in particular the elite unit Detachment 88 which is relatively small but highly trained in intelligence-gathering, investigative and forensic techniques and has a track record of success. In July 2004, with Australian support, the Jakarta Centre for Law Enforcement Cooperation (JCLEC) was opened in Jakarta to provide “a resource for the Southeast Asian region in the fight against transnational crime,

with a focus on counter-terrorism.” Among other work, it helps co-ordinate and facilitate a range of training programmes, including seminars and workshops.

The Philippines: As with Indonesia, there are several organisations in the Philippines engaged in counter-terrorism work. At national level, primary responsibility rests with the National Intelligence Co-ordinating Centre (NICA) which is answerable to the Prime Minister’s Office. In Mindanao and the Sulu Archipelago, the military intelligence service is responsible for providing intelligence support for counter-insurgency operations.

Thailand: Thailand has several agencies focused on counter-terrorism, these include the National Intelligence Agency (NIA), the Royal Thai Police Special Branch (Santhiban) and Army Intelligence. The Internal Security Operations Command (ISOC), a military-controlled organisation established in the 1960s to combat communist insurgency, has recently assumed a role in combating separatist insurgency in the south of the country.

Association of Southeast Asian Nations (ASEAN):

Established in 1967, ASEAN has recently started to move in the direction of helping member nations coordinate strategies on “transnational crime and international terrorism.” While it is still defining the role that it can play, a number of significant milestones have been passed. In January 2006, a “Treaty on Mutual Legal Assistance in Criminal Matters” was signed by all members and has thus far been ratified by five, and more recently in January 2007, ASEAN leaders signed the “ASEAN Convention on Counter Terrorism” (ACCT).

INFORMATION FOR NON-LOCAL BUSINESSES

For non-local businesses investing in Southeast Asia and seeking more information, their first port of call should be their foreign ministry website and from there they will be directed to their local embassy or high commission. The British Foreign & Commonwealth Office and the American State Department have also established two very useful organisations under their respective foreign services that offer detailed reports for national firms, but also offer some open information on their websites:

• **Security Information Service for Business Overseas (SISBO) www.sisbo.org.uk**

A unit based in the Foreign and Commonwealth Office but funded by the private sector, SISBO is the first point of contact for UK businesses trying to assess the current threat to their business operations outside the United Kingdom. The website acts as a one-stop shop for British business to obtain

background briefings on specific countries where there is both significant commercial opportunity and a lack of understanding of the business risks. SISBO’s future plans also include the creation of a subscriber service that will share more detailed reports, drawn primarily from declassified government sources.

• **Overseas Security Advisory Council (OSAC) www.osac.gov**

OSAC is an organisation run by the Diplomatic Security Service of the US State Department to support American business around the globe. As well as posting regular reports and briefings on their public website, they run ‘Country Councils’ in 122 different countries to act as information-sharing groups on security matters. OSAC and SISBO also run occasional joint conferences on security matters around the world.

Beyond these official outlets, it is recommended that business managers also seek private assistance in assessing the specific risk that they may face to an investment or operation. Advice can be provided by academic institutions, private security contractors and risk analysts.

An aerial photograph of a densely populated urban area, likely in Asia, showing a mix of high-rise buildings and lower residential structures. The entire image has a teal or cyan color tint. Overlaid on the upper left portion of the image is a large, bold text block.

**RISK MANAGERS SHOULD
HAVE SOME AWARENESS
OF THEIR PROXIMITY TO
POSSIBLE TARGETS**



3. Positive and holistic mindset: Adopt security as part of corporate culture and regard good security practice as a business enabler, not a hindrance.

The principles listed here are universal. Enshrine security within corporate structure and planning. As with all other aspects of business, the Board of Directors should take the lead in ensuring that security is factored into all aspects of the business. There are a number of basic things that security officers and other senior executives should bear in mind when considering the physical location of a business. In looking around your buildings and considering building and staff expansion plans you should consider the following:

Who are your neighbours? While your actual business might not be directly threatened, you may be right next door to (or on top of) a station or building that is, and the impact of collateral damage must be borne in mind.

Design security in: The threat from terrorism should be a consideration in the design and construction of any new building or facility, especially large glass structures in city centres. It is a great deal easier, cheaper and more effective to incorporate security into a design at the outset than it is to “retro-fit” security to a facility whose design has not taken account of this issue. Well-designed security features can actually enhance both the functionality and aesthetic appeal of buildings without adding to their cost.

How secure is your building? Are the main entry and exit points securely guarded? A regular review of the ease with which people can enter and exit your building either unimpeded or unseen is essential. For example, underground car parks are an often overlooked potential security threat. This does not require a fortress mentality, but regular reviews will enshrine the importance of security among staff.

Who is working for you? While strengthening vetting procedures is unlikely to stop the most determined individual, consistently applied procedures to verify that individuals are who they say they are (through production of birth certificate, passport, references or other official documentation) will strengthen the defences of a business at a basic level.

Have a “Safe Room”: Terrorists draw inspiration from Al-Qaeda tactics and their preference is for multiple and simultaneous attacks. This often means that evacuating a building in the most obvious direction is not necessarily the safest option, as evacuated staff might simply be moving into

the path of another bomb. Calculate where the safest room in your building is, ensuring that it has as few glass windows as possible, and if possible use that as the rallying point for staff in the event of a terrorist alert.

Test your evacuation plans: In much the same way that fire drills should be run regularly, a regular evacuation test is a good idea.

Business continuity plan: Most businesses and organisations now have some kind of business continuity plan, but not all organisations exercise the plan periodically or amend it in the light of experience or changing circumstances. There is much advice available from governments and the private sector about how to plan business continuity and disaster recovery, but while the expertise to build a plan can be acquired externally, the plan itself needs to be owned by the organisation. In particular, ensure you have an alternate site that is sufficiently far from your main location and think through how staff currently get to work.

Emergency contact system: Communication is essential in times of emergency. Make sure you have updated contact information for all of your staff and ensure that systems are in place for staff to check in regularly if they are leaving the home base for an extended period of time.

Prepare for the threat of cyber-terrorism, and the hijacking of business websites by terrorists.

The threat from cyber-terrorism is relatively low but cannot be discounted entirely. A more immediate risk is from cyber-criminality. As the average age of terrorists falls, and a generation educated with computers rises through the ranks, the importance of technology to their campaign grows. The possibility of innovative ways to damage business through cyber-terrorism must always be borne in mind, and for the most part a strengthening of existing cyber-security measures offers effective protection. Below are some key points to consider:

Which critical systems are computer controlled?

Which basic critical systems in your building are computer controlled, and who oversees them and their security?

Who are you hiring? The biggest threat to computer security comes from insiders with legitimate access to corporate systems. How good are your vetting systems and are procedures being followed?

Who is using your site and mainframe? Who is using your site? How regularly do your IT team check for hidden intruders?

Consider the threat from chemical, biological, radiological and nuclear (CBRN) attack.

The chemical, biological, radiological and nuclear (CBRN) threat is not easy to quantify, and ill-founded scare stories abound. Al-Qaeda has expressed ambitions to acquire these capabilities both for their destructive potential and, more importantly, because of the fear factor a successful CBRN attack would induce. However, there is so far no evidence that Al-Qaeda or any group affiliated to it has succeeded in developing or acquiring any CBRN capabilities, and these capabilities are not easy to acquire or to deploy. Of the available options, the one most likely to succeed is a radiological or “dirty” bomb, using conventional explosive to scatter radioactive material. The use of anthrax is another strong possibility and in the longer term, the increasing proliferation of biotech scientific expertise and the facilities to do it will make bioterrorism a more substantial threat. The consensus view from the global security and intelligence community is that sooner or later a CBRN attack will take place in one form or another. From the business perspective, the most encouraging news is that effective general security measures of the type outlined earlier in this chapter offer the best defence against this form of attack. Some additional points to consider are laid out below:

Is your mail scanned? Electronic devices that perform such tasks can be prohibitively expensive for smaller businesses. However some basic training for mailroom staff can enable them to stop to verify the provenance of suspicious or unexpected packages and help isolate potentially dangerous mail away from the bulk of staff. Such basic training can also help protect from the potential threat of letter bombs.

Does someone know how to turn off your ventilation?

Such a basic piece of training is critical to ensure that an airborne pathogen or chemical is not allowed to spread through your building. Making sure that individuals on staff know how to turn off the ventilation is an easy way to minimise the risk to staff and also shortens the clean-up time afterwards.

Do you have emergency breathing apparatus for all staff?

For smaller businesses, this can prove to be a prohibitively high expense. Some basic training can show staff how they might protect themselves using more mundane items from around the office.

4. Understand and protect your supply chains.

Standard good business practice should be to know and understand exactly how your supply chain functions. These basic pointers should help a risk manager assess exactly where the weak points are:

What does your supply chain look like? Where exactly do all your products come from and where do they all go? What does the actual map look like? Having a visual understanding of this is crucial when considering how safe it is.

Are there any “chokepoints”? Are there any points along your supply chain that if shut down would bring you to a stand-still? Can alternative routes be established, either for permanent use, or in the event of an attack upon one point?

Are you reliant on others for elements along your supply chain? Have you discussed contingency plans with them? Have you identified alternatives in the event that they become targeted?

Have you backed-up electronic networks? Control of many supply chains is automated; have you considered a back-up system in the event of cyber-penetration or an attack to crash your mainframe? Who oversees or is responsible for your cyber-security?



ORGANISATIONS
SHOULD ADOPT
SECURITY AS PART
OF THE CORPORATE
CULTURE

**CONSIDER WHETHER
YOUR INVESTMENT
DECISIONS AND
EMPLOYMENT POLICIES
CAN BE USED TO HELP
MITIGATE THE THREAT**

5. Engage with the wider business community, government and society on the issue of terrorism and security.

Regional governments in Southeast Asia take the threat of terrorism seriously and have done a lot to mitigate it. They cannot offer total assurance against this threat though and it is in the interests of companies to consider what they can do to help themselves and society as a whole. Your home nation's foreign ministry may be able to help, but it may also be worth seeking out what other firms have done. They may be able to help you achieve a better understanding of specific local circumstances or developing innovative and effective technical solutions to mitigate particular threats.

Take a long-term strategic view and consider whether your investment decisions and employment policies can be used to help mitigate the threat. This could involve:

- **Promoting diversity within the workplace and hiring local staff.** Taking steps to ensure that your local staff's legitimate needs are catered for and that they are made to feel welcome and valued – such “smart HR” policies will not only help in the long term, but in the short term it will also likely help mitigate the threat from within.
- **Taking great care to make sure that language in any formal documents or statements is used sensitively.** This will of course vary from nation to nation, but taking care to make sure that your statements are phrased in such a way as to not offend will undoubtedly help your company's local image.
- **Engaging in local community projects.** Small sums of money or pro-bono work can make a big difference for your company's image locally. This cannot buy immunity from attack. But such activity can play an important role in shaping the environment and reducing the appeal of radical propaganda among local communities.

Be aware of the global dimension of Islamist extremism.

Singaporean Prime Minister Lee Hsien Loong has defined the threat in Southeast Asia as follows: “In countries with large Muslim populations, there are small minorities at the fringes who are inclined toward extremist views and terrorist methods. Globalisation and easy foreign travel enabled them to come into contact with extremist teachings of militants abroad, and to become part of an international network.” And beyond training, the ideologies espoused by these groups become global in their perspective. This is particularly relevant to companies with overseas operations, including within the Islamic world. One way of looking at Islamist extremism is as a reaction to a process of globalisation widely perceived as having benefited the West to the detriment of Islamic societies. A greater sense of cultural awareness and readiness to engage with local communities as delineated above will help deflate the Islamist rhetoric internationally.

**CAREFUL FORWARD
PLANNING WILL HELP
BUSINESS **MANAGE**
THE THREAT MORE
EFFECTIVELY**

CONCLUSIONS

As with the terrorist threat faced anywhere in the world, the root causes and effects of terrorism in Southeast Asia are deeply localised. However, what business can do to both mitigate the threat and ensure that it is contributing in a positive way to countering local radicalisation is fundamentally the same around the globe. Basic resilience messages about protecting your business from outside threats are as applicable in Southeast Asia as anywhere else, and good business practice, embedded in a deep awareness of local cultures and traditions, will help ensure that business is helping rather than hindering local government efforts to stem terrorism.

Ultimately, the key lessons to draw from this report are:

1 THERE IS NO NEED TO RE-INVENT THE WHEEL

Most of the resilience strategies to help business counter the terrorist threat posed in this region are extensions of established good practice globally

2 TREAT SECURITY AS A BUSINESS ENABLER

When thinking for the future, be it HR policy, building location and design, or expanding abroad, consider the threat from terrorism early on in planning rather than retro-fitting

3 'SMART HR'

Not only in terms of protecting yourself from the 'threat within', but also in terms of helping more broadly with the struggle that we face through a proactive approach to diversity. A 'smart HR' policy should be the foundation of any businesses structure

4 TEST YOUR SYSTEMS REGULARLY

It is all very good having a well developed business continuity plan, but it needs to be updated and tested regularly to ensure it is still valid and applicable. In the same way fire drills should be done regularly and tests of other protective measures should be tried and tested

5 UTILISE EXISTING KNOWLEDGE

Be it local or international research institutions, international security or risk analysis firms, government sources, or even the local security services, it is worth ensuring that you have touched base with more than one of these sources before you make a decision to invest in a specific part of the world.

No amount of planning will ultimately ever completely eliminate the threat from terrorism. However, careful evaluation and preparation will help business manage the threat more effectively and will ensure that your organisation is able to continue operations following an attack. Moreover, such resilience will strengthen the message that society as a whole rejects the terrorist effort to disrupt and alter our economy and our way of life.

APPENDIX

INSURGENT AND SEPARATIST GROUPS IN THE SOUTHEAST ASIA REGION

This table does not purport to be a comprehensive list of all insurgent and separatist groups in Southeast Asia. Only groups thought likely to pose a current threat have been included.

INDONESIA

Group	Area of operations	Aims/remarks
Front Pembela Islam (Islamic Defenders Front) (FPI)	Indonesia	Strict Islamic organisation supporting the implementation of sharia law within the current government framework.
Mujahideen KOMPAK	Central Sulawesi, Indonesia	To establish Islamic government in Indonesia; Jemaah Islamiah splinter group.
Organisasi Papua Merdeka (OPM)	Indonesia	Political organisation seeking independence for West Papua.
South Maluku Republic/Republik Maluku Selatan (RMS)	Eastern Indonesia	Christian separatist group fighting for Maluku (Molucca) independence.

PHILIPPINES

Group	Area of operations	Aims/remarks
al-Khobar	South Cotabato province	Similar ideology to Moro Islamic Liberation Front and Jemaah Islamiah, envisaging the establishment of an Islamic state in South Philippines.
Kabataang Makabayan (KM) /Nationalist/Patriotic Youth	Philippines	Student wing of the Communist Party of the Philippines opposing the existing government.
Moro Islamic Liberation Front (MILF)	South Philippines	Independent Islamic state in Bangsa Moro and neighbouring islands. Currently on a ceasefire.
Moro National Liberation Front (MNLF)/Bangsamoro Army	South Philippines	Muslim separatist movement fighting for the establishment of an Islamic state in South Philippines. A peace accord was signed with the government in 1996. Various MNLF splinter groups currently operate in the area and are believed to be linked to the Abu Sayyaf Group.
New People's Army (NPA)	Rural Luzon, Visayas and Mindanao	Armed wing of Communist Party of the Philippines (CPP) aiming to overthrow the existing government. Ended peace talks with the government after 1999 Philippine-US agreement to resume joint military exercises.
Revolutionary Proletarian Army–Alex Boncayao Brigade (RPA–ABB)	Manila, central Philippines	Urban hit squad Communist Party of the Philippines (CPP). Embraces anti-globalisation ideology.

Tactics/weapons

Conduct yearly raids during the month of Ramadan.

Bombings, murder and decapitation.

Limited rebel insurgency; small-scale raids and attacks.

Small bombings.

Main targets

Night clubs, bars, gaming halls and other venues considered “not respectful of the holy month”. Attacked Playboy magazine in 2006 by throwing stones at the Jakarta office.

Religious targets. Responsible for bombing a church in Jakarta (2001), killing 17 Christian villagers (2003), and decapitating three Catholic schoolgirls (2005).

Indonesian officials, military installations, and foreigners. Notable was the attack against a weapons depot in 2003. Notable attack against a weapons depot in 2003.

Government targets. Blamed for several small attacks. Suspected of bombing the Maluku Governor’s office in 2002.

Tactics/weapons

IEDs, bombings and extortion.

Active in student protests

Bombings, small arms, large shootings of civilians, kidnapping, torture.

Kidnapping and murder.

Intimidation, extortion, assassination.

Small arms (grenades and automatic weapons).

Main targets

Private citizens and property targets.

The single major violent attack was the 1971 hijack of a Philippine Air Lines domestic flight to China.

Private citizens and property, business targets and transport. Despite the ceasefire, the latest attack was reported in early 2007 when MILF bombed a fast-food chain in Cotabato.

Private citizens, business and religious targets. MNLF has a long history of kidnapping priests. One of the latest major incidents attributed to MNLF was the seizure of over 100 civilian hostages in Zamboanga in late 2001.

Foreign investors and foreign businesses, Philipino politicians, security officials and the media. The latest attack was the assassination of the leader of a local association in Sorsogon in 2007.

Government and economic targets. Fight against the NPA. A few attacks against the Department of Energy were reported in 2000.

APPENDIX

INSURGENT AND SEPARATIST GROUPS IN THE SOUTHEAST ASIA REGION CONTINUED

This table does not purport to be a comprehensive list of all insurgent and separatist groups in Southeast Asia. Only groups thought likely to pose a current threat have been included.

THAILAND

Group	Area of operations	Aims/remarks
Barisan Revolusi Nasional (BRN)	Southern Thailand	Muslim separatist movement fighting for the establishment of a pan-Malay independent Republic of Pattani. Possibly linked to JI, KMM and GMIP.
Pattani Islamic Mujahideen Movement / Gerakan Mujahideen Islam Pattani (GMIP)	Southern Thailand	To establish a Muslim state in Southern Thailand. Group has possible links to JI, Al-Qaeda, KMM, Barisan Revolusi Nasional.
Pattani United Liberation Organisation (PULO)	Thailand	Separatist insurgents fighting for the separation of Thailand's mainly Muslim south.
Runda Kumpulan Kecil (RKK)	Southern Thailand	Seek an independent state for Pattani.
United Front for the Independence of Pattani / Bersatu	Thailand	Umbrella group including PULO, New PULO, and BRN wanting to establish an independent Islamic state in southern Thailand.

TRANSNATIONAL GROUPS

Group	Area of operations	Aims/remarks
Abu Sayyaf Group (ASG)	South Philippines, Indonesia	To establish an independent Islamic state in west Mindanao and Sulu - split from Moro National Liberation Front (MNLF).
Al-Qaeda	International; Philippines, Malaysia, Singapore, Indonesia	"Re-establish the Muslim state" worldwide. International network controlled by Osama Bin Laden. Known to carry out suicide attacks. Connected to numerous groups globally and financed by drug trafficking, ID theft and fraud. <i>No Al-Qaeda active cells are believed to be present in the region but there exists a track record of Al-Qaeda operatives using Malaysia and Thailand as transit and facilitation points.</i>
Jemaah Islamiyah (JI)	Malaysia, Indonesia, Philippines, Singapore, Thailand	To establish an independent Islamic state encompassing southern Thailand, Malaysia, Indonesia and southern Philippines.

Tactics/weapons

Arson and robbery.

Small-scale shootings and arson attacks.

Bombs, IEDs, small arms and arson.

Bombings.

Soft attacks (IEDs and arson) avoiding large armed clashes.

Tactics/weapons

Bombings, IEDs, kidnappings, assassinations, beheadings, rapes and extortion. The group appears to have moved away from its original aim and has started operating as a purely criminal organisation.

Suicide attacks, car bombs, bombings, IEDs, kidnappings, assassinations.

Suicide attacks, car bombs, bombings.

Main targets

Government and police force and other “symbols of Thai repression”. In a coordinated attack, 18 government-run schools and two police posts were set on fire in 2004.

Muslim leaders and institutions opposing Wahhabism .

Schools and police targets.

Attacks predominantly against government targets. Known for staging simultaneous bombings.

Business targets (banks) and Muslims who cooperate with the Thai government.

Main targets

Private citizens and property, business, journalists/media. The group has been involved in terrorist attacks throughout 2007. In May 2007 a cell planning attacks on public areas was uncovered in Manila.

Private citizens and property, foreigners, commercial targets, utilities, police and security forces, government, transport. No recent Al-Qaeda linked attacks have been reported in the region.

Tourist targets, private citizens and public sites, eg markets. JI is suspected of having had a role in the 2005 Bali bombings that resulted in the death of 20 people. Also notable was a car bomb attack in 2004 in which 202 people died and 300 were injured.

**GOOD BUSINESS
PRACTICE, EMBEDDED
IN A DEEP AWARENESS
OF LOCAL CULTURES
AND TRADITIONS,
WILL HELP ENSURE
THAT BUSINESS IS
HELPING RATHER THAN
HINDERING LOCAL
GOVERNMENT EFFORTS
TO STEM TERRORISM**

Disclaimer

This document is not a prospectus or invitation in connection with any solicitation of capital. Nor does it constitute an offer to sell securities or insurance, a solicitation or an offer to buy securities or insurance, or a distribution of securities in the United States or to a US person, or in any other jurisdiction where it is contrary to local law. Such persons should inform themselves about and observe any applicable legal requirement.

Whilst every effort has been taken to verify the accuracy of this information, neither the International Institute of Strategic Studies, Lloyd's nor their affiliates can accept any responsibility or liability for reliance by any person on this information.

Copyright Notice: © 2008 the International Institute of Strategic Studies and Lloyd's. All rights reserved.



Since merchants first met to insure their ships at Edward Lloyd's coffee shop over 300 years ago, nearly every aspect of the way we do business has changed. But one constant is the bold confidence proclaimed by our motto, reflected in both our unique appetite for risk and our worldwide reputation for settling valid claims.

