



Terrorism Risk Management Strategies for BUSINESSES

Terrorism, like any other risk, demands a strategy of active risk management for all businesses. As in-house counsel, you should position yourself at the vanguard of ensuring your company's protection from terrorism and its consequences. Although relatively rare, terrorism can no longer be assumed to be of negligible probability even in the United States, and in certain markets, it is commonplace. Your risk management strategy and corporate contingency planning must reflect this reality, taking into consideration not only your company's legal and moral responsibility to employees and stockholders, but also the primary and secondary consequences of terrorist activity upon the whole business. This article will discuss the current atmosphere of terrorist threats and will address various ways that you can help your company protect itself from suffering either a terrorist attack or its consequences.

Today's terrorists appear likely to seek commercial targets and to maximize casualties and physical destruction. The attack of September 11, 2001, upon New York's financial community was grave enough in loss of life, interruption of business, and the cost of recovery, but imagine the implications of the use of even a small "dirty bomb"—radiological material packed around conventional explosives—in the same area of Lower Manhattan. Civilian casualties from the explosion itself and resultant exposure to radiation could easily be on a par with 9/11, but the bomb would also force the closure of a swath of the city for many months for decontamination. Businesses without designated alternative sites would risk losing access to critical data for a period so prolonged that their survival would be in serious jeopardy.

**By William F. Waite and
David S. Claridge**

Reprinted with permission of the author(s) and the American Corporate Counsel Association as originally appeared: William F. Waite and David S. Claridge, "Terrorism Risk Management Strategies for Businesses," *ACCA Docket* 21, no. 8 (September 2005): 74–89. Copyright © 2005 William F. Waite, David S. Claridge, and the American Corporate Counsel Association. All rights reserved. For more information or to join ACCA, call 202.293.4105, ext. 360, or visit www.acca.com.



William F. Waite is the chief executive officer and general counsel for The Risk Advisory Group Ltd., for which he was a founding director in 1997. Before founding The Risk Advisory Group, he was a case controller for the UK government's Serious Fraud Office. He is available at bill.waite@riskadvisory.net.



Dr. David S. Claridge is the managing director for Janusian Security Risk Management Ltd., the security risk management subsidiary of The Risk Advisory Group. Before joining Janusian, he helped to establish the Centre for the Study of Terrorism and Political Violence at the University of St. Andrews. He is available at claridge@janusian.com.

THE THREAT TO BUSINESS

One of the most challenging decisions for any business seeking to offset risks with controls is how to allocate resources for risks that are low in likelihood but potentially catastrophic in consequence. For companies whose operations are predominantly located in and focused upon the United States, Western Europe, Australasia, and Japan, terrorism risk falls into the category of low probability—high consequence. Even for companies operating in countries with a higher likelihood of terrorism, such as Colombia, Israel, or the Philippines, the chances of terrorism seriously affecting operations are relatively low in comparison to, say, wider political risks or that of serious information technology (“IT”) failure caused by a computer virus.

In a recent survey of the UK’s top 500 listed companies, company finance directors and senior managers placed terrorist risk as their lowest concern out of a list of 12 business risk categories.¹ A separate survey of security and risk managers at 50 inter-national corporations revealed that 63 percent see terrorism as a significant threat to their organization.² What’s more, 72 percent believed that the threat to their organization would increase over the next 12–24 months, despite data subsequently published by the U.S. State Department showing that, in 2002, the number of recorded international terrorist incidents fell to the lowest ever figure of 199 attacks, a 44 percent drop from that of previous years.³

But the bland supposition that, because it happened once, it will happen again does not adequately address the specific threat to business. There are clear signs that al Qaeda’s leadership viewed the global economic effect of the 9/11 attacks as a considerable bonus and consequently adjusted its rhetoric to encourage its constituent groups and supporters to carry out further actions against trade and commerce. Post-9/11 attacks by al Qaeda have focused on private sector targets.

In addition to their economic attractiveness, private sector targets also offer a practical advantage as governments make their buildings more secure. Risk managers need to be cognizant of the fact that, if their business appears to be an easy target, there is a much greater chance of terrorists exploiting that vulnerability. According to the U.S. State

Even with detailed contingency plans and supplementary data sites, your company would probably have its back to the wall over the sheer financial burden of loss of operations and physical costs of cleanup in the aftermath of such an attack. Insurance coverage for terrorism has been very hard to come by in New York since 9/11, so many companies there have had little choice but to self-insure. There has been considerable question over the capacity of international reinsurance markets, which paid \$30–\$58 billion following 9/11, to cope with a second comparable loss, with the result that the United States introduced the Terrorism Insurance Risk Act of 2002 to provide financial backing to the insurance industry. There is a real danger that claims will not be honored as insurers go under from the loss. What’s more, you will find that almost every terrorism insurance policy excludes chemical, biological, radiological, and nuclear (“CBRN”) varieties.

These facts raise serious issues for in-house counsel. The potentially catastrophic nature of radiological or chemical terrorism means that different rules need to be in place in terms of emergency management and recovery planning, as well as handling the massive cleanup costs that would be involved. You must grasp the extent to which your business will need financial and physical resilience in the aftermath of an act of terrorism, perhaps at a level of severity that we have yet to experience.

Department, 51 percent of international terrorism in 2002 was against business targets. For a quick discussion on assessing the risk of terrorism, see the sidebar at right, and for a more in-depth discussion of risk analysis, watch for the article devoted entirely to that topic in the November/December 2003 *ACCA Docket*.

Although the successful post-9/11 attacks have predominantly occurred in developing countries, more than 15 developed plots have been uncovered in North America, Western Europe, and Southeast Asia. It would be wrong to assume that, because the security and intelligence services of the developed world have managed to prevent a catastrophic terrorist act on their collective soil since 9/11, they can continue to do so forever. It would be equally incorrect to assume that groups connected to al Qaeda will consider only prestige targets, such as government buildings or major events. Furthermore, it is just as plausible that supporters of al Qaeda will attack in Boise as in New York City, and there is an equivalent level of threat in Western Europe.

Companies must not underestimate the extent to which terrorism has become a truly global phenomenon. Terrorism risk is manageable, but it must first be assessed and understood, followed by active steps to protect assets, people, reputations, and long-term survival of businesses.

MANAGING THE TERRORIST THREAT TO BUSINESS

Every business presents a unique profile in terms of its nationality, geographic exposure, size and revenue, internal risk management structures, publicity and brand exposure, need for open doors, the makeup of its workforce, and its appetite for risk. Despite these variances, it is possible to provide general advice to in-house counsel who should seek to define the framework under which the threat from terrorism is addressed, both to ensure that corporate duty of care is fulfilled and that measures are being taken to reduce exposure to future legal, as well as physical, risks.

Although many of these measures are independent and protective in nature, businesses are responsible for participating in the fight against terrorism. In part, this responsibility means ensuring compliance with legislation and regulations intro-

duced since 9/11, including the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act ("USA PATRIOT Act"). It also means taking

ASSESSING RISK

Risk is a term that is widely used, but frequently with an imprecision that can be confusing and misleading. Risk is not the same thing as *threat*, nor is it a synonym for *probability*. Instead, assessing risk is the process of considering how the world around us may affect us and shaping our behavior and resource allocation accordingly.

An effective security risk assessment requires evaluating at least three components: threat, vulnerability, and effect.

- **Threat:** Threat refers to what the group or individual can do to harm your company, and part of assessing that threat is to look at the motivation and capability of terrorists in general or a particular group that you think may want to attack your company. By considering both capability and motivation, you can develop a picture of how people may seek to exploit vulnerabilities. You can then make judgments about the likelihood of such events occurring.
- **Vulnerability:** Keeping in mind your findings from your threat assessment process, you need to then take the next step of considering where security vulnerabilities lie. After you have completed this step, you may need to assess how to plug any holes that you may have uncovered in your security systems and operational planning.
- **Effect:** Effect refers to what an incident involving a particular threat, such as in this case terrorism, will cause to happen. In business terms, you need to understand the potential effect of each threat upon continued activity. You should then design your company's security plan to counteract those threats and to most rigorously protect processes that are critical to your company's success and survival.

By combining these judgments in a risk matrix, you can make more effective decisions concerning allocation of resources for the mitigation of risk.

active steps to ensure that businesses do not unwittingly act as havens for terrorist sympathizers or conduits for their funds. Dialogue and collaboration with government agencies are critical if businesses are to play their part in countering the terrorist threat, and in-house counsel can play a central role not only in ensuring compliance with the bare minimum requirements, but also in communicating with government officials.

BE RESOURCEFUL AND CREATIVE IN GATHERING INFORMATION, BUT BE CAREFUL TO ANALYZE THE POTENTIAL NEGATIVE EFFECTS OF HAVING YOUR COOKIES FALL INTO GOVERNMENT, TERRORIST, OR INDUSTRY WATCHDOG HANDS.

From Intelligence to Action

Actively managing risk means having access to two critical categories of information:

- What are we trying to protect?
- What is the threat to us?

As in-house counsel, you should play a key role in ensuring that the right people within your organization are asking these questions. Addressing them requires two processes to be in place:

- Thorough profile of your organization, examining the nature of your company's exposure along the lines suggested in the introduction to "The Threat to Business" section above.
- Regular reviews of intelligence relating to the terrorist threat, on a timetable determined by the profile.

Responsibility for the review process is likely to vary among organizations, but businesses should place intelligence gathering at the base of the organization, supplemented by efforts from senior risk managers to make informed judgments from a corporate perspective. Information may be gathered from a variety of sources, including local and international press, local workforces, contact with embassies and local officials, the FBI's Awareness of National Security Issues and Response ("ANSIR") program, and the State Department's Overseas

Security Advisory Council ("OSAC"), as well as commercial risk databases and advice. For a list of such sources, see the sidebar at right.

The culture of government openness in the United States makes liaison with intelligence and law enforcement agencies relatively straightforward. Elsewhere, such is not always the case. In the UK, for example, liaison with the Security Service is restricted to the largest companies or those working in particularly sensitive sectors.

You should use all of the government contacts at your disposal, because the information provided by the government can be quite useful and because it usually has been collected and collated with a degree of rigor. Government sourcing, however, is not critical to a successful intelligence-gathering operation. Most intelligence is available in open source, and certainly, most information required to make strategic security judgments is in the public domain. Be resourceful and creative in gathering information, but be careful to analyze the potential negative effects of having your cookies fall into government, terrorist, or industry watchdog hands, and then consider adding the following steps to your research strategy:

- Check out terrorist websites. Most terrorist groups have websites although many have been taken down by the authorities since 9/11. Some experts suggest regular visits to any remaining sites. Others, however, warn that, unless you're absolutely sure that no government agency will come down on you for regularly visiting terrorist websites, you may want to collect your information in other ways.
- Read internet newsgroups and mailing lists to gauge the views of particular communities. Again, the same caution as above: Some experts say to visit any remaining sites regularly. Other experts, however, warn that, unless you're absolutely sure that no government agency will come down on you for regularly visiting terrorist websites, you may want to collect your information in other ways.
- Use human sources as widely as possible. For example, speak to local government officials and your own employees.

In practice, an ideal intelligence structure within a typical multinational corporation may be established as follows:

From this point on . . .

Explore information related to this topic.

ONLINE:

- ACCA's committees, such as the International Legal Affairs Committee, the Law Department Management Committee, and the Small Law Departments Committee, are excellent knowledge networks and have listservs to join and other benefits. Contact information for ACCA committee chairs appears in each issue of the *ACCA Docket*, or you can contact Staff Attorney and Committees Manager Jacqueline Windley at 202.293.4103, ext. 314, or windley@acca.com or visit ACCA OnlineSM at www.acca.com/networks/ecommerce.php.
- Centre for the Study of Terrorism and Political Violence, at www.st-andrews.ac.uk/academic/intrel/research/cstp/.
- Civil Contingencies Secretariat (UK), at www.ukresilience.info/home.htm.
- Department of Homeland Security, at www.dhs.gov.
- FBI Awareness of National Security Issues and Response, at www.fbi.gov/hq/ci/ansir/ansirhome.htm.
- *Homeland Security*, an ACCA InfoPAK available on ACCA OnlineSM at www.acca.com/infopaks/homeland.html.
- International Policy Institute for Counterterrorism, at www.ict.org.il/.
- Jihad Unspun (pro-Islamist site), at www.jihadunspun.com.
- Overseas Security Advisory Council, at www.ds-osac.org/.
- Possible Indicators of al Qaeda Surveillance, at www.asisonline.org/newsroom/dhsbulletin032003.doc.
- The Security Service (UK), at www.mi5.gov.uk.
- Separatist, Paramilitary, Military, Intelligence, and Political Organizations, at www.cromwell-intl.com/security/netusers.html.
- Terrorism Research Centre, at www.terrorism.com.
- David B. Zoffer and John J. Donlon, "Developing a Crisis Management Plan," *ACCA Docket* 18, no. 8 (September 2000): 18–31, on ACCA OnlineSM at www.acca.com/protected/pubs/docket/so00/crisis.html.

ON PAPER:

- ANONYMOUS, *THROUGH OUR ENEMIES' EYES: OSAMA BIN LADEN, RADICAL ISLAM AND THE FUTURE OF AMERICA* (London: Brasseys, 2002).
- ROHAN GUNARATNA, *INSIDE AL QAEDA* (New York: Columbia University Press, Reissue 2003).
- BRUCE HOFFMAN, *INSIDE TERRORISM* (New York: Columbia University Press, 1999).

AT ACCA'S 2003 ANNUAL MEETING:

- Are you looking for even more information on this topic? If so, plan to attend ACCA's 2003 Annual Meeting October 8–10 at the San Francisco Marriott. Visit www.acca.com/education03/am to learn more about the meeting and register by August 29 to save \$\$.

If you like the resources listed here, visit ACCA's Virtual LibrarySM on ACCA OnlineSM at www.acca.com/resources/vl.php. Our library is stocked with information provided by ACCA members and others. If you have questions or need assistance in accessing this information, please contact Staff Attorney and Legal Resources Manager Karen Palmer at 202.293.4103, ext. 342, or palmer@acca.com. If you have resources, including redacted documents, that you are willing to share, email electronic documents to Managing Attorney Jim Merklinger at merklinger@acca.com.

- Local offices monitor information around them, such as from local press and contact with law enforcement agencies and embassies, and send a brief daily or weekly update to corporate risk management.
- Corporate risk management monitors international developments in the press, uses a commercial intelligence company, subscribes to OSAC's email list, and monitors the FBI ANSIR and Department of Homeland Security websites. Risk management then assesses the significance and reliability of both this and locally sourced information.
- Corporate risk management tests the information against three questions:
 - Does any information suggest that we are a specific target or that we fall into general categories that may make us vulnerable?
 - How might terrorists think about us in light of current events?
 - How might terrorists try to target us, and what are they capable of?
- Corporate risk management then uses the answers to these questions to form a view of local threats and the exposure of the business at a moment in time and to determine future intelligence requirements.

SECURITY IS INCOMPATIBLE WITH NORMAL LIFE—BY ITS VERY NATURE, SECURITY IS INTRUSIVE, DISRUPTIVE, AND OBSTRUCTIVE.

On the basis of this intelligence cycle, risk managers can provide advice to local offices and traveling staff. This process can be formalized into alert states, perhaps on a digestible scale from low to extreme or green to red, that reflect the company's perceived threats at corporate and local levels. Typically, the alert state will link into a series of predetermined security procedures. For example, your company could decide that, at alert state red (high), all nonessential travel would be restricted and all vehicles entering company premises would be subject to search.

Planning for Terrorism

Terrorists seek vulnerabilities that will allow them easy access to their targets. The attacks of 9/11 exploited a clear weakness in the security around domestic aviation in the United States. Reducing the opportunities for terrorists to get close to targets will have a proportionate effect on the frequency of successful attacks or will at least push terrorists away to less well protected locations. To a considerable degree, this result has already started to happen, as governments have hardened security and terrorists have been forced to consider commercial facilities as an alternative. Consequently, corporate risk managers must make a priority of pushing terrorism away from their doors.

From a corporate perspective, planning for terrorism has two components:

- Establishing flexible security plans that can be adjusted according to the perceived threat level.
- Embedding appropriate emergency response, disaster recovery, and business continuity plans to allow the business to cope with an attack.

Security Planning

Security is incompatible with normal life—by its very nature, security is intrusive, disruptive, and obstructive. Our call for the establishment of an intelligence network at the core of a corporate counterterrorism program reflects this understanding. The close relationship between intelligence and security is described perfectly by the former director general of the British Security Service (MI5), as follows:

It is most important that protective security measures result from intelligence, so that it is the things which are genuinely vulnerable which are being protected. Otherwise security can become an industry in itself and will not be protecting what is truly at risk.

Unfortunately, there is frequently an inadequate connection between intelligence and protective security measures, resulting too often in measures being put into place after the event and then gradually wound down in a comparatively short space of time when nothing further happens, in response to complaints of delays or inconvenience.⁴

Corporate security planners should take heed of these words. Security measures must be allowed to move up and down in response to adequate assess-

ments of threats and in accordance with an established plan.

The contents of a security plan will vary considerably from corporation to corporation, but should include consideration of the following issues:

- **Physical security:** Refers to gates, fences, barriers, locks, and other forms of access control associated with providing physical obstacles to entry to property. Most of this equipment takes some time to source and fit and thus is not always suitable for scaled fitting and removal according to threat level. Many businesses prefer to prefit appropriate security around access points and bring them into service only during increased alert states. This approach, however, may undermine one of the most beneficial qualities of physical security, which is its deterrent effect: if a building looks like a fortress, it is much more likely that an assailant will select a softer target. Different businesses have varying tolerances for physical security. Retail premises, for example, must be open to the public to continue functioning, while industrial facilities can afford to provide more substantial physical measures. Businesses should be prepared to introduce the maximum level of physical security possible while continuing their core activities and scale downwards, rather than scaling up at short notice.
- **Guard force management:** Security guards are a critical link in increasing the flexibility and reach of physical security. Guards should combine static activity around entry points and irregular patrolling to identify suspicious activity and breaches. Guards are generally the weakest link in any security system, despite their vital function, because they are usually significantly underpaid, undertrained, and undermanaged, often as a consequence of being operated by an outside supplier selected on the basis of price rather than quality. You might want to take your guard forces back under the direct employ of your company in order to control their management and training more effectively. If you do use outside suppliers, consider concentrating their use for providing short notice reinforcements, training for employed staff, and performance monitoring.
- **Closed-circuit television (“CCTV”) and alarm systems:** Companies are increasingly using electronic systems to supplement or replace guard force patrolling. You can use digital recording systems to place virtual “masks” over areas covered by cameras and then to establish camera patrolling. In such a system, movement within a masked area triggers a camera to cover it and sounds an alarm. You can then readily enhance digital images and use available software to allow facial recognition against a database in a split second. You can combine CCTV with a small quick reaction force to reduce the need for human patrols and monitor security for “intelligent buildings” from a remote control room, sometimes hundreds of miles away. In countering terrorism, high quality CCTV images operated by a trained and attentive security guard can be vital in identifying patterns of hostile surveillance outside a perimeter or in public environments, such as shopping centers or sports games. Too often, however, companies leave CCTV completely unmonitored and rely on it only for evidential purposes after a crime has been committed. CCTV is useful as a deterrent only if it is watched actively by someone trained to know what to look for and if it is integrated into a wider security plan.
- **Search frequency and procedures:** During periods of heightened threat, your security plan should allow for searches of people, possessions, and vehicles at the outer perimeter of a building. At the highest alert state, every vehicle entering a cordon should be searched. At lower alert states, the frequency may drop to 1 in 5 or 1 in 20 vehicles, depending upon traffic flow and the need for unhindered vehicle movement. In areas where speed of movement is required, your company could use airport style metal detector arches, detector wands, and X-ray machines.
- **Staff training and briefings:** The active participation of all staff in a raised level of awareness of possible terrorism threats is perhaps the most significant component in the counterterrorism strategy. Because the eyes and ears of staff are everywhere, you should encourage all employees to report suspicious activity and to challenge anyone or anything out of the ordinary. Consequently, it is important to ensure that your staff is aware of the current alert state and that they behave accordingly. It is also important that staff have

appropriate training to allow them to deal with security incidents. The nature of the training will vary according to role. For example, a receptionist should receive instruction in dealing with bomb and other threats made by telephone or in person, whereas a member of your Middle East sales team may need a more comprehensive course in local threats, personal security, and evasive driving techniques. A course with the following components is ideal for most general needs:

- Briefing on threats in region of interest or internationally (as required).
- Personal security advice.
- Vehicle security advice.
- Interpersonal conflict resolution techniques.
- Fear and stress management.
- Antisurveillance and countersurveillance techniques.
- Hostage survival skills.

In addition to general training, wherever possible, staff should be regularly briefed on matters of security, either at a regular staff meeting, on the corporate intranet, or through a newsletter.

- **Staff levels and activities:** At times of heightened security, your company should consider whether it is necessary to expose all staff to the risk of terrorism. For overseas offices, this decision is likely to mean requests for dependents to leave the country or for nonessential staff to do the same. In some cases, a complete evacuation may be ordered. Security plans should reflect the need to reduce exposures and to protect people in different configurations from the norm.
- **Travel management:** In any large organization, it is difficult to know precisely who is where and when, all of the time. Many corporations now run travel management systems, under which staff must certify that they (1) have appropriate knowledge of their destination country and the threats that it contains, (2) have completed security awareness training, and (3) have entered travel details into a database that records their itinerary. Your company should make sure that tickets are not issued and not available until after these commitments have been made.
- **Close protection:** For high-profile executive staff or those operating in particularly hostile environments, the permanent presence of trained close protection operatives provides some relief from

security concerns and helps to deter some terrorist groups. Effective close protection does not always require large teams of operatives. It is often sufficient to consider one security manager to simply take the strain of thinking about security concerns to allow company staff to carry on their activities without having to expend effort on the issue.

IF A COMPANY CAN DEMONSTRATE THAT IT HAS TAKEN REASONABLE SECURITY MEASURES BASED ON AN ACTIVE ASSESSMENT OF THREAT, IT CAN MORE LIKELY PREEMPT POSTINCIDENT ACCUSATIONS OF NEGLIGENCE OR INATTENTION.

There is no magic solution to mitigating terrorism risk. The above measures fulfill one or both of two purposes: (1) to deter terrorists by making it harder for them to get close to buildings and staff and (2) to allow security staff to identify and respond to suspicious activity. Al Qaeda has taken operational planning to new heights by indulging in meticulous preparation, including detailed surveillance on potential targets. Herein lies the network's real weakness. If security staff can identify terrorists during the planning phase, prophylactic measures can be put into place by local security forces. The importance of this situation has been recognized by the U.S. government, which has issued advice to businesses on identifying terrorist surveillance. See the sidebar on page 81 for a link providing information on possible indicators of al Qaeda surveillance.

Crisis Planning

Not even a perfectly executed security plan can provide total protection from terrorism, and businesses can be situational victims rather than direct targets. You, as in-house counsel, must understand this reality, because security planning plays a part in managing the expectations of staff and board members, which in turn has implications for litigation risks if the company becomes a victim of terrorism.

Security needs to be balanced against the need to continue commercial activities, and what is good for protection against terrorism is not always good for business. If a company can demonstrate that it has taken reasonable security measures based on an active assessment of threat, it can more likely preempt postincident accusations of negligence or inattention. For example, make sure (1) that your company has in place the following routine security measures and (2) that your company routinely monitors and enforces these security measures every day and not just when the threat alert level rises:

- Appropriately clear all new hires, such as with background checks.
- Use appropriate technical security, such as antivirus software.
- Train personnel as to what to do if a threat occurs.
- Adopt a sanction policy with teeth in it for breaches of security and actually openly enforce the security policy.
- Institute effective termination procedures, such as retrieving keys and blocking computer access.

MOST MAJOR COMPANIES NOW HOLD KIDNAP-FOR-RANSOM INSURANCE FOR EXECUTIVE STAFF, BUT ALL SHOULD CONSIDER HOW THEY INTEND TO RESPOND TO A KIDNAP EVENT THROUGHOUT THE LABOR FORCE.

It is equally important that you can demonstrate that your company has plans to protect staff and to minimize the physical and wider effects of a terrorist attack. Contingency planning for security crises traditionally falls into three categories:

- **Emergency response:** Procedures for dealing with the immediate effects of an incident, with the primary purpose of ensuring the safety of employees.
- **Business continuity:** Plans for ensuring that core business activities can continue in the event of disruption or loss of one or more sites.

- **Disaster recovery:** Returning the business to its normal operating capacity in spite of losses suffered.

Such plans have wide applicability, covering such disaster events as fire or generalized IT system failure. There are, however, some particular issues raised by terrorism as opposed to these other events.

A critical difference between most crisis events and those relating to terrorism is the issue of moving people in response to a warning or an attack. In a fire, for example, plans almost always provide for evacuation. Terrorist attacks are much less predictable, and evacuation is not always the best option. Imagine a crowd being hustled into the street in response to a bomb threat when it explodes next to them or inside the building, forcing shards of glass out into the crowd. Depending on building layout, invacuation or moving people to a strengthened area inside may be preferable. If the building does not have a suitable invacuation area, plans will need to be established for searches before the need for evacuation arises to establish secure zones well away from buildings. CBRN events also require specific plans for invacuation, sealing of entry points, and shutting down of air conditioning and ventilation systems.

Terrorist events also require special attention to liaison with law enforcement and first responders. Information is likely to be confused, and responders are likely to be heavily overstretched. Particularly in the event of CBRN terrorism, plans should adhere to the advice offered by the British government to “go in, stay in, tune in”: limit movement and follow official advice broadcast by the media. Businesses should give specific consideration to their response to CBRN attacks, particularly with regard to establishing zones for the decontamination of people. If company security officers are to contain the inevitable panic that would follow such an event, they will need to be able to demonstrate a semblance of control over the situation. This requirement means having established systems of communications, command, and control and includes having established prior liaison with local law enforcement.

Companies must also prepare for other tactics employed by terrorists. Most major companies now hold kidnap-for-ransom insurance for executive staff, but all should consider how they intend to

respond to a kidnap event throughout the labor force, especially in those countries where law enforcement may respond to dubious motivation. Businesses with representation in high-risk countries must establish evacuation plans. Careful consideration must be given to the categories of staff that companies are prepared to evacuate—all senior staff, all Americans, all expats, everyone? Consideration must also be given as to what will serve as a trigger for an evacuation. Equally, consideration must be given to the logistics of evacuation: if you are going to fly people out, where to? Where will they be accommodated when they arrive? Do you have the financial resources readily available to effect a short notice evacuation? Will flights even be available, and what are the alternatives if they are not? Planning must reflect consideration of and reasonable attempts to come to terms with these dilemmas.

OUR INTERCONNECTED ECONOMIES AND SOCIETIES OFFER MANY OPPORTUNITIES FOR TERRORIST EXPLOITATION IN PLANNING AND CONDUCTING ACTS OF VIOLENCE: INTERNATIONAL BANKING AND FINANCE, GLOBAL TRANSPORT AND LOGISTICS, HIGH SPEED MASS COMMUNICATIONS, AND CHEAP, WIDELY AVAILABLE TECHNOLOGY.

In terms of continuity and recovery planning, responding to terrorism is less differentiated from other categories of threat. Preparation should reflect the worst case: complete loss of buildings, perhaps even loss of use of sites if a CBRN weapon has been used, and the loss of large numbers of staff. Alternative sites must be in locations that are suitably removed from existing sites and should be more than skeletons, because they may form the backbone of the business for a prolonged period. Continuity plans should reflect not only the physical loss that your company may suffer, but also the

financial ramifications of shifting stock markets and closed markets. The attacks on 9/11 demonstrated how quickly markets can contract following a major terrorist incident.

At every level of the contingency plans, the central concerns must be to ensure that roles are allocated appropriately and with clarity, that the company has the resources to back up its plans, and that key staff have been trained in the execution of their roles and preferably have participated in at least one simulated exercise. Experience in managing the aftermath of terrorist incidents is hard to come by, and the effect of CBRN terrorism is a complete unknown. It is important that businesses seek to embed the knowledge that is available into their business processes now to allow time for plans to settle in, for simulations to be run, and for identifying weaknesses.

Fighting Terrorism

On September 14, 2001, a London *Times* editorial summed up the mood of the time: “We are all counter-terrorists now,” it bristled, acknowledging the reality that the public sector cannot defeat terrorism on its own. Modern terrorists are predominantly private sector operators, using civilian channels to conduct paramilitary actions. Our interconnected economies and societies offer many opportunities for terrorist exploitation in planning and conducting acts of violence: international banking and finance, global transport and logistics, high speed mass communications, and cheap, widely available technology. As private rather than public sector investment and innovation has driven the global capitalism model, it is inevitable that the private sector will hold the key to arresting the exploitation of these tools by malevolent forces.

The primary motivators for the private sector, however, are revenue growth, greater market share, maximal profits, and shareholder value, none of which is especially compatible with layers of extra bureaucracy and overhead associated with long-term anti- and counterterrorism measures. Such legislation as the USA PATRIOT Act and the Anti-Terrorism, Crime and Security Act in the United Kingdom have sought to force companies to take a more active part in understanding with whom they do business and to provide greater assistance to intelligence and investigative authorities.

Unfortunately, government is often very clear in its broad agenda, but misses the detail that is necessary to make regulations workable. This discrepancy has been particularly true in the case of U.S. and UK post-9/11 legislation, which has placed a considerable burden upon businesses, often under threat of considerable sanction. This burden has introduced an area of risk for businesses that was previously absent: the regulations themselves. Efforts at partnerships that combine incentives, as well as sanctions, such as the U.S. Customs Trade Partnership against Terrorism, have had some success, but businesses continue to complain that they are overburdened with responsibility.

For your business to participate most effectively in countering terrorism, you need to consider a number of actions:

- Routinely screen all new staff to confirm background data.
- Undertake due diligence on all partnerships and suppliers, especially in high-risk markets.
- Implement extra financial controls in high-risk markets.
- Retain communications records as long as allowed by local law.
- Pursue prosecution of illegal use of brands and counterfeiters, who potentially feed money into terrorism.
- Establish effective liaison with law enforcement and report activity of interest to them.

CONCLUSION

The low probability of terrorism may appear to suggest a risk management strategy that emphasizes planning, recovery, and maintenance of continuity over active intervention. But terrorism can have catastrophic potential and, to some degree at least, can be deterred. Fairly unsophisticated security measures play a critical part in persuading terrorists to turn their attentions elsewhere. Solid contingency plans are an important foundation, but regular reviews of risk levels are vital.

The 9/11 attacks highlighted the need for businesses to insulate themselves from the financial effect of terrorist attacks upon them. In planning for terrorism risk, companies would do well to link up terrorist threat assessment and financial plan-

ning with legal and compliance departments to ensure that a consistent and coherent terrorism risk management strategy is in place.

BUSINESSES THAT FAIL TO ADDRESS THE TERRORISM ISSUE ARE FAILING TO UNDERSTAND THE ABILITY OF THE NEW BREED OF INTERNATIONAL AND LOCAL TERRORISTS TO STRIKE ANYWHERE AND MAXIMIZE THE EFFECT OF THEIR ACTIONS.

Terrorism is a long-term threat. Businesses that fail to address the terrorism issue are failing to understand the ability of the new breed of international and local terrorists to strike anywhere and maximize the effect of their actions. The proven desire of al Qaeda operatives to access and use weapons of mass destruction is a case in point. Even the most robust businesses would struggle to survive the loss of a major headquarters and its staff. Responding to these challenges requires imagination and collaboration with law enforcement and intelligence bodies, as well as with other companies working in comparable fields or geographic areas. By sharing information and advice and by making their physical and human assets as inaccessible as possible, companies can take positive steps to reduce their exposure to terrorism risks. ■

NOTES

1. The Institute of Chartered Accountants and The Risk Advisory Group, *Managing Risk: Views of Senior Directors of the FTSE 500*, at www.riskadvisory.net/hyperlinks/views_dir/views_dir.html.
2. *Janusian-RAND Terrorism Survey*, unpublished document, presented to private conference, Apr. 1, 2003 (copies available from authors on request).
3. U.S. STATE DEPARTMENT, PATTERNS OF GLOBAL TERRORISM 2002 161 (2003).
4. Stella Rimington, *Terrorism Did Not Begin on September 11*, THE GUARDIAN, Sept. 4, 2002.