A. C. Macris Consultants

UPDATE

Vol III Issue 03-05

Highlights

This article is the second in our ongoing series of Leadership, Business, and Terrorism. In our first article we presented the case for understanding the risks and vulnerabilities that terrorism presents to business leaders and introduce the concept that terrorist threats have added a new dimension to business leadership. This article goes to the next level where we define the types of threats as Direct or Indirect. We further break the Indirect threats into three categories of (1) an act of terrorism against a key client , (2) an act of terrorism that severely depresses one or more client industries, and (3) acts of terrorism against a company's supply or logistic chain, including shipping, etc.
The discussion provides a background into the direct and indirect impacts of terrorism, and identifies some of the critical factors that must be considered to arrive at a well-defined risk profile for any business or operation.
Our next article takes our research and develops the specifics of our Integrated Business Risk Profile (IBRP), its individual components, and demonstrates how these components should be evaluated to maximize risk reductions for a given level of investment.

UPDATE is published quarterly by A.C. Macris Consultants. UPDATE's charter is to provide interesting articles, on timely topics, authored by people in industry, academia, or business.
Please contact us at the following:
Telephone: 860.572.0043
E-mail: acmpc @ acmacris.com
U.S. Mail: P.O. Box 535, Mystic, CT 06355

Leadership, Business and Terrorism
The Ripple Effect

by:

Ozzie Paez
Simplicity Data Systems

A. C. (Dean) Macris
A. C. Macris Consultants

The first article in this series introduced the new demands placed on business leaders by the emerging risks in this age of evolving terrorist threats. This article moves the conversation forward, focusing on the first related test of business leadership in protecting the business from terrorism: addressing terrorist threats to the organization and understanding the total threat picture, which includes direct and indirect threats. This point is worth reinforcing, no business can expect to address the risks of terrorism if its senior executives do not understand its nature, source and impact on the business and the economy. While most business executives understand direct terror related risks (hijacking, bombs, etc.), many do not fully comprehend indirect risks, their potentially devastating impacts and much higher probability of occurrence. The effects of this knowledge gap can result in inadequate protective measures and ineffective recovery strategies, the impacts of which would be magnified during a national or international crisis. Specifically, the exclusion of indirect risks will likely translate into inadequate risk analysis, incomplete business recovery plans, ineffective business continuity plans, and poor preparation for the effects of government initiated actions, as happened following the attacks on New York and the Pentagon. The effects of poor preparation can extend all the way to core business functions that include capital investments, supply chains, inventory, customer diversity, and acquisitions.

This paper outlines the roles that effective business leaders should play to protect their investments and those of their shareholders from the direct and indirect effects of terrorism. These include leading the organization into areas that, prior to 9/11, were traditionally handled further down the corporate structure, including ensuring that threats-risks are clearly defined and understood at the highest level of the organization, and that effective plans are developed and put in place to ensure sustainable operations following a major terrorist event.

Images of 9/11, Madrid, and now London vividly illustrate the direct impact of a major terrorist event. While the direct impacts of these criminal acts are easy to appreciate, very few business leaders truly understand the ripple effects of these events and how extensive those effects can be. The following sections were crafted to help our readers improve their level of understanding of the ripple effects of these events and their indirect impact on business operations.

Direct Effect

The direct effects of terrorist events on public and private facilities, population centers, transportation systems and social institutions are powerful and clear to see, as 9/11, Madrid and London tragically illustrate. Images of mass casualties, destruction of property and damage to highly symbolic targets such as warships (USS Cole), the World Trade Center, embassies, and the like flash in our minds when we first hear of a new threat or actual terrorist attack. While these are high impact targets, carrying significant personal, emotional and financial consequences, the probability of any individual target getting hit is relatively low and

is even lower for less attractive targets, i.e. an individual manufacturing facility, small town or specific shopping mall. The difficulty is in figuring out precisely how low those probabilities are and how significant the impacts of a given incident are likely to be. To help illuminate this issue, we will drill down into the hierarchy of potential terrorist acts and explore their consequences taking into account that as higher visibility targets become hardened, terrorists will progressively look to softer ones with the potential for significant impact on local communities and the national economy.

Our analysis will start with the next level in the hierarchy, which will focus on a particular industry, contrasting it to the likelihood of attack against a specific target. The probability of a terrorist act against a particular industry is much higher than that against any individual target, even a high visibility one, particularly when the high visibility target has improved its security posture. To wit, the tactic of flying a commercial airliner into a skyscraper is known, the authorities have instituted policies, procedures and training that heighten awareness, enhance security, and reduce the probability of occurrence. So for the purposes of this discussion, for a particular industry, the likelihood and impacts of a terrorist act are highly contextual, i.e. dependent on a set of context specific variables. To illustrate this point we will use the cruise ship industry as a reference, assuming an act of terrorism is perpetrated against a large cruise ship.

The impact of a terrorist attack on the cruising industry can be predicted to be similar to those on the airline industry following 9/11, with one major contextual difference, the cruise ship business does not provide a necessary service – taking a cruise is optional for almost all of the industry's customers. People don't use cruise ships to get from one place to another in a timely efficient manner, and businesses (a primary consumer of travel services) do not rely on cruising for transportation. Thus, cruising should be categorized as very discretionary, and if people feel unsafe or vulnerable then they are likely to spend their vacation money elsewhere. Therefore, the ripple effects and impacts of a terrorist attack on the future of the industry most probably would include a steep decrease in passenger load, expanded security regulations, added costs for screening and other security measures similar to what airlines are required to perform, less convenience for passengers, an overall decrease in quality of customer experience and the potential of a government imposed shut-down period to allow for security upgrades to be instituted. Here again, the industry's unique context works against it in a number of important ways. First, unlike airplanes, whose purpose is to get passengers to a destination, cruise ships are both transport and destination, either in part or in total, depending on whether passengers disembark at destinations along the way. Thus, while the pilot and crew have significant latitude in controlling the environment within an airplane, the crews on ships must not become a nuisance or impediment to movement by passengers. The bottom line for this industry is that any attack on a cruise ship is likely to trigger immediate and potentially long term, severe impacts measured in reduced bookings and increased operating costs.

Third Party Direct Effects

Drilling down further, let's consider a direct act of terrorism against a third party, using assets obtained legally or illegally from another party or industry. Traditional security prior to 9/11 focused on protecting company assets from damage, intentional, accidental and Acts of God. The events of that tragic day raised awareness of another type of risk, the use of company assets to attack a third party. In his case, the assets of two companies, American Airlines and United Airlines, were used to attack third parties, the World Trade Center and the Pentagon. Now, industry had to consider the possibility of equipment (airplanes, trucks, ships, etc.), hazardous materials, information and even employees being cooped by terrorists not to damage the company, but to attack others. This has severe implications for many companies that use, manufacture, package and ship materials useful in conducting attacks, as well as those operating shipping and road/rail transportation systems.

When we assess the probability of terrorists obtaining assets from a specific company, it appears to be very low, but when considered in terms of a company within a given industry involved in particular activities – for example, companies that ship radioactive medicines and sources – the risks are much higher and the impacts will not be limited to the affected companies. In this context, risks will spread across that industry and potentially others, with likely government involvement, higher regulatory burdens and related operating cots. In this context, risk calculation must include higher probability of occurrence, particularly in terms of an industry as a whole, very high financial impact through civil actions, potential of criminal sanctions for failure to adequately guard assets, shutdown of all or most operations for a significant period of time, increased government scrutiny (as with airlines following 9/11), and, of course, new regulations. For companies involved in international trade, these types of events can cause shipments to be delayed at the source, in transit and leaving/entering ports as governments react to unexpected terrorist events.

In the Direct Effect context, it is relatively straightforward to understand the vulnerabilities as well as the consequences of terrorism, although the third party effects described above are not always obvious to the untrained mind. The discussion now continues with a more subtle and less understood (although equally significant) type of impact, what we define as the Indirect Effects of Terrorism.

Indirect Effects

Traditional risk management practices were built around mitigating incidents and recovering from threat events, manmade or accidental. The previous section discussed the direct risk category in the context of terrorism, while this section focuses a category not often considered in developing an organization's risk profile, Indirect Effects. When we speak of Indirect Effects we generally refer to three general areas or subcategories: (1) an act of terrorism against a key client or clients, i.e. an attack on a cruise ship, whose company is an important client, (2) an act of terrorism that severely depresses one or more client industries, i.e. the airline, travel and hotel industries in the aftermath of 9/11, (3) acts of terrorism against the supply or logistic chain, including shipping containers, telecom, etc., which would either significantly raise costs, cut margins or disrupt operations/production. When discussing these three categories there are assumptions. Perhaps the most important assumption is that the level of exposure increases from category one to three. That means the number of opportunities for disruption are non-linear and more complex.

Acts of terrorism against a key client

For this subcategory, the primary consideration is the number of important business clients and the probability that one or more of them will be affected by a terrorist attack. While this category has the potential for the greatest direct effects, the probability of a specific act of terrorism against a particular business or small group of businesses, in the absence of other factors, is very low. The high impact of the ripple effects, should such a low probability event take place, is due to the likely loss of business from the targeted client as it struggles to get back to operations, assuming that recovery is possible at all, thus the effects could range from short term to the permanent loss of the client and its business.

Acts of terrorism against an industry of key clients

In this situation we consider the impact of a terrorist attack on the overall industry or industries represented by the target(s) of the attacks. The classic situation is the airline industry in the immediate aftermath of the 9/11 attacks. Consider the multitude of downstream businesses that were affected by the 9/11 attacks, i.e. travel, tourism, hotels, restaurants, and amusement parks. Now consider the scope of critical industries and their high visibility targets within the overall U.S. economy, from chemical plants to rail transportation. By shifting the focus from individual facilities to overall industry segments, the probability that a terrorist attack will affect specific businesses increases substantially. As mentioned above, this argument is based on overall exposure for an industry as opposed to specific facilities and the cascading indirect effects of an attack. When considering the potential indirect effects of a terrorist attack on an industry, downstream businesses that support the target industry must consider the likely loss of business from key client(s), who were directly or indirectly affected by the attacks. These clients will in turn be affected by loss of business (as experienced by airlines after 9/11), disruptions and shifts in focus from the need to comply with new requirements and regulations, and reduced operating margins affecting expenditures in the short and mid-term. Finally, the same scenario described above can affect key clients of a business, as opposed to the business itself, as the effects cascade down the economy, adding to the overall impact in varying degrees.

Acts of terrorism against the supply or logistic chain, including shipping containers, telecom, or others

This is the third and most complex subcategory in that it considers the effects of an attack that could disrupt access to materials and services, therefore disrupting the ability of the business to produce and deliver its products or services. The factors within this subcategory are many and a full listing is beyond the scope of this newsletter, but in general they include disruptions in the supply of raw materials, components, systems and financial support services. The impacts can be minimal where alternative sources of supplies or services can be quickly identified, however, where unique services or low volumes of custom supplies are involved (such as in Just-In-Time inventory systems) the effects can be catastrophic. On the other side of the equation is the ability of the company to get its goods to market, which is particularly critical for short shelf-life products such as fruits and produce. In the indirect context, examples of this category include:

- Terrorism against containers or the container shipping ports, which disrupt the ability to export or import products,
- Contamination of the food supply resulting in the disruption of foodstuff distribution and exports,
- Shutdown of ports and import/export facilities,
- Disruptions in transportation systems required to ship goods to market, i.e. airlines, rail and trucking,
- Disruptions in raw material production such as oil, coal and natural gas,

The primary variables of attacks at this level are time, criticality and alternative sources of critical supply chain services. If a company has no plans and must formulate a strategy post-event, then those companies that do have a plan are likely to absorb remaining capacity of existing critical services, products and materials. The law of supply and demand, combined with the likely involvement of brokers (speculators) is likely to affect available capacity and inventories, which will translate into delays and much higher prices, as evidenced by the energy crunch in California a few years ago and the high costs of crude oil in today's market.

> Images of 9/11, Madrid, and now London vividly illustrate the direct impact of a major terrorist event. While the direct impacts of these criminal acts are easy to appreciate, very few business leaders truly understand the ripple effects of these events and how extensive those effects can be.

Dr. Stephen Flynn outlined the high vulnerability of key supply chain links in his book *America the Vulnerable*. His work and our research demonstrate that any disruptions to the logistics chain are likely to have a significant ripple effect across multiple industries and, in some cases, throughout the world economy. The projected impacts and the large numbers of supply chain components throughout the world economy justifies our consideration of this subcategory as one of high probably and maximum impact.

In Summary

The discussion above provided a background into the direct and indirect impacts of terrorism, and identified some of the critical factors that must be considered to arrive at a well-defined risk profile for any business or operation. The table below summarizes the category and discussion, providing an overview of the approach and methodology used by our organization to assess threats and risks, and to define effective ways to mitigate them. We committed at the start of this article to develop the case for systematically delineating and understanding the risks and consequences of terrorist acts, thereby allowing senior corporate executives to craft policies and develop plans to mitigate risks and ensure sustainable operations. We trust that we have met that objective through a threat-risk based framework and hierarchy, which clearly captures the overall impact of terrorism on markets and businesses, while providing a deeper understanding of the relationship between specific attacks and total effects.

We have been able to prepare this perspective because our team has spent many years researching the effects of terrorism, drawing on many decades of experience in the military, government and with large organizations. Discussing research and delineating

problems is important to understanding how to deal with the challenges. Therefore, what does our work and research mean to you and your business? Specifically, How can we help government, military, companies and political leaders to better understand and respond to direct and indirect threats?

By assisting them in:

- Enhancing awareness, understanding and engagement of senior executives in an area previously left to managers and staff,
- Establishing a framework for assessing threats-risks over the long term, as conditions change,
- Defining an integrated threat-risk profile that integrates the direct and indirect effects of terrorism,
- Identifying options for mitigating risks and metrics to ensure effective Returns on Investments,
- Updating business security assessments and security, continuity and recovery plans to integrate necessary components of terrorism,
- Identifying strategies for 'balancing risks' through client portfolio, financial investments and project controls.

In our ongoing series on the topic of Leadership, Business, and Terrorism, we recognize that we must continue to move from the conceptual and almost academic discussion of these issues to more tangible 'take action' position. In our next article we will discuss the Integrated Business Risk Profile (IBRP) and its individual components, and demonstrate how these components should be evaluated to maximize risk reductions for a given level of investment.

Threat Event	*Probability*	*Impact*	*Drivers*
Direct			
Attack on my organization	Very low	Very high	Attractiveness of target, location, industry…
Indirect			
Attack on my industry	Much higher	Significant	Critical industry that might have a broad, visible impact
Attack on key client	Very low	Very significant	If perceived to be an attractive target only
Attack on key client industries	Much higher	Very significant	Disruption of an industry
Attack that impacts my logistic chain	Much higher	Very significant	Broad impact on several industries or infrastructure such as financial systems

P.O. Box 535 Mystic, CT 06355
www.acmacris.com