

September 15, 2003

Thwarting terror: Protecting the Shareholders' Investment

Continued inaction could yield economic disaster

September 11, 2001. Two years later, the date still sends shivers of dreadful recollection through Americans from coast to coast. The scarred landscape in lower Manhattan, the hole in the skyline—the visual and emotional vestiges of those attacks serve as potent reminders that the United States faces an enemy bent on its destruction.

Last July, the government released a declassified report describing the results of a joint inquiry into U.S. intelligence activities before and after the September 11 terrorist assaults. Produced by the U.S. Senate Select Committee on Intelligence and the U.S. House Permanent Select Committee on Intelligence, the document summarizes the history of the terrorist threat against the United States and the rise of Osama bin Laden and his al Qaeda organization. The committees disclose intelligence reports that offered clues to a massive assault planned for spring or summer 2001, although no firm evidence revealed the exact timing or nature of the attack. Without casting blame on the federal agencies involved, the report identifies systemic weaknesses in the U.S. intelligence community that contributed to the successful execution of the simultaneous assaults in New York and Washington, D.C., and the aborted attempt that ended in Pennsylvania.

Twenty-four months later, these weaknesses remain; more importantly, the nation's enemies remain committed to their exploitation. No major attack has occurred on U.S. soil during that time, but history assures that plans for the next wave are well underway. The government and private sectors alike must prepare to deflect a future terrorist strike—or face retribution from a betrayed American public.

Evolution of terror

Since September 1979, *The Lipman Report* has provided in-depth coverage of the terrorist threat against the United States. That menace has changed drastically during the last quarter century.

Earlier reports focused on kidnappings and executive protection, hijackings and bombings. These threats primarily affected American interests overseas, but in 1981, the government formed a Senate subcommittee to investigate the possibility of terrorist acts on U.S. soil. Twenty years before the fall of New York's World Trade Center, members of the

Subcommittee on Security and Terrorism worried that failure to curb the threat of domestic and foreign terrorism would enable the problem to overwhelm the United States as it had other countries.

Terrorist attacks against the United States in the 1980s and early 1990s painted terrorism as a primarily state-sponsored phenomenon. The government viewed these groups as instruments of their sponsors, motivated by regional or issue-related interests. These organizations had not aimed for mass casualties, and while they threatened U.S. persons, interests and assets, the U.S. homeland itself appeared safe from their reach.

Two seminal events in 1993 marked the beginning of a new era in terrorism: the February bombing of the World Trade Center and the June arrest of conspirators in a foiled plot that targeted several New York landmarks, including the United Nations and the Lincoln and Holland tunnels. Both plans aimed to kill thousands of innocent civilians and involved groups comprised of multinational members acting without a state sponsor. Another important change was the focus on America and on attacking symbolic targets within the United States.

Osama bin Laden and his connection to international terrorism reached the attention of the U.S. intelligence community in the early 1990s. The Central Intelligence Agency learned in 1993 that bin Laden was financing Egyptian extremists and in 1994 that al Qaeda was supporting terrorist training camps in Sudan. Identified by an al Qaeda defector as the head of a global terrorist network, bin Laden exhorted followers to wage war against Western military targets in the Middle East in 1996, after he found a haven among the Taliban in Afghanistan. He expanded this *fatwa*, or religious decree, in 1998 to include U.S. military and civilian targets anywhere in the world—even the U.S. homeland.

A patient, resourceful enemy

A few months later, two truck bombs destroyed U.S. embassies in Kenya and Tanzania, killing

(continued on next page)

Thwarting terror: Protecting the Shareholders' Investment

Continued inaction could yield economic disaster

(continued from preceding page)

224 and injuring 5,000. The timing of these attacks—just weeks after a press conference in which bin Laden discussed “bringing the war home to America”—may have suggested an immediate response to the *fatwa*, but they resulted from years of careful planning. In fact, these bombings demonstrated several disturbing traits that distinguish the terrorist threat of al Qaeda from the state-sponsored groups of the 1980s.

The subsequent investigation revealed that the embassy bombings in East Africa took place five years after the dual attack was conceived. Likewise, the attack on the *USS Cole* in October 2000 involved years of planning. Al Qaeda's proclivity for careful, patient plotting marked a significant change from other terrorist groups. For this reason, law-enforcement officials remain convinced that the seeds for the September 11 assault on the World Trade Center were sown in 1993, with the failure of the first bombing.

The September 11 attacks and the 1998 embassy bombings demonstrate another characteristic typical of this new breed of terrorism: the ability to execute simultaneous attacks. Few terrorist groups have enough skilled planners and operators to coordinate such sophisticated operations, making multi-pronged assaults rare.

This point raises yet another distinction between al Qaeda and other groups: size. Most terrorist organizations are relatively small, with fewer than 100 dedicated members. Even at its height during the 1970s and 1980s, the Irish Republican Army did not exceed 400 activists. By contrast, al Qaeda has tens of *thousands* of people at its disposal, trained in terrorist camps in Sudan and Afghanistan. Only a small percentage have pledged their loyalty to bin Laden himself, but the rest are committed to accomplishing the organization's objectives.

Despite the size of the al Qaeda network, bin Laden's followers maintain tight operational security, compartmentalizing the details of specific plans to minimize the risk of disclosure. Operatives

receive instructions strictly on a need-to-know basis. Intelligence agencies thus have a difficult time disrupting the group's activities, even if they succeed in capturing and interrogating low-level members. Similarly, foiling one plan will not necessarily reveal information about other plots also in progress.

Other trademarks of this modern terrorist threat include flexibility and creativity. Traditionally, terrorists have used small arms and conventional explosives. The bombing of the *USS Cole* and the September 11 attacks displayed imagination and strategic flexibility. The command structure of al Qaeda shows similar versatility and employs several modes of operation, including: tasking skilled fanatics with a mission; training laypeople to execute simple, but deadly, attacks; and assisting local groups with their own activities.

Target: the U.S. economy

Such is the nature of the new terrorist threat: patient, cunning and deadly. Yet, much of the country believes the danger has passed.

The threat remains, and it has targeted the lifeblood of the modern world: the U.S. economy.

Just as Hitler revealed his murderous designs in *Mein Kampf*, so has bin Laden publicly declared his goal as the destruction of the American economy—a message repeated in numerous video, audio and written statements. In one audiotape, the terrorist mastermind praises the executors of the September 11 attacks for inflicting \$1 trillion in economic damage. He continues the message by telling his followers that economic annihilation holds the key to their victory over the United States.

Indeed, striking government and military targets would wreak colossal damage and chaos, but it would not produce an economic meltdown. That deathblow would require al Qaeda's forces to assail the civilian companies that drive the economic engine, putting at special risk the industries making up the nation's critical infrastructure,

those physical and computer-based systems essential to operating the economy and government. These sectors include telecommunications, energy, banking and finance, transportation, water systems and emergency services, among others, and are primarily controlled by private enterprise.

The joint inquiry report focuses on ongoing, systemic weaknesses in the U.S. intelligence community, a body whose primary mission lies in national security. Far more unprepared are the private-sector companies concerned mainly with profitability in the turbulent economy of the last two years; for many of these organizations, security budgets have dwindled even below pre-September 11 levels. Too many businesses have taken a myopic approach to security, believing that they cannot afford to invest in systems and procedures to defend against an apparently “phantom” threat.

To see the danger of such erroneous thinking, one need only look at the U.S. aviation industry.

In 1996 President William J. Clinton created the White House Commission on Aviation Safety and Security. The commission proposed a \$1.1 billion anti-terrorism plan that dedicated \$350 million to enhancing airport security. Recommendations included broader installation of explosives-detecting machines, a full bag-to-passenger match on domestic flights at selected airports and development of an automated passenger profiling system. The commission also called for tighter screening of airport and airline employees and more uniform security standards. In the end, however, the aviation industry largely ignored the commission’s proposed security measures, citing such factors as cost, privacy rights and passenger inconvenience.

On September 11, 2001, terrorists exploited several well-documented weaknesses to hijack four airliners. In the two years since, two of the nation’s three major airlines have filed bankruptcy, with the third in peril of following suit. The

industry’s suppliers have suffered similar financial consequences. “Industries pay a price when they fail either individually or collectively to address known vulnerabilities,” warns a national security expert, “because someday someone will come along and use those vulnerabilities, and the industry will suffer financially.”

Enacting the commission’s recommendations in 1996 may well have averted tragedy five years later. The industry’s decision to save the expense of increased security ultimately proved “penny-wise and pound-foolish.”

‘Expect the unexpected’

No one can predict when or where the next attack will occur. The members of the joint inquiry concede that more effective handling and processing of received intelligence would not necessarily have prevented the tragedy of that multi-pronged assault. High-level government reports and private assessments identify countless weaknesses in the national security program. Plugging every conceivable hole could literally consume the country’s entire gross national product and require decades for implementation.

Accepting this reality, however, does not mean that organizations can ignore the problem and blindly hope the threat materializes somewhere else. The entire nation shares the responsibility for protecting itself against this dangerous, but still human, enemy. The government and private sectors must first acknowledge the severity of the modern terrorist threat and then dedicate the resources necessary to preserve their operations.

Expect the unexpected. Instead of attempting to defend against a specific type of attack, businesses need to study the capabilities of their prospective opponents and their own weaknesses. This advice applies not only to terrorism, but also to more commonplace security concerns, such as corporate or industrial espionage, workplace violence or even simple theft. Companies must identify their

(continued on next page)

Thwarting terror: Protecting the Shareholders' Investment

Continued inaction could yield economic disaster

(continued from preceding page)

vulnerabilities and determine the potential costs of exploitation. The security program should then rank those weaknesses according to their relative impact on the organization; remediation plans begin with the liabilities that could have the greatest effect on business continuity.

Take a holistic approach to security. Uniformed security officers, access-control procedures and closed-circuit television cameras are important elements of an effective security program, but a broader view can identify significant shortcomings. Background screening—not only of employees, but also of vendors and temporary personnel—can help protect an organization against infiltration by “sleepers,” agents who integrate themselves into society until called to action. When selecting business partners, companies must conduct due diligence in investigating potential suppliers, considering such factors as their vendors, facilities and customers.

Develop a risk management strategy. Companies need to include security in their board- and senior-level risk-management strategy. Typically covering such areas as competitive action, the financial markets and insurance, the strategy should also quantify the cost of preventing a security incident. What is the likelihood that a specific threat will occur? What are the projected costs associated with a successful breach? Such proactive planning can help organizations determine the most effective way to allocate their security budgets, while demonstrating the measurable value of the security investment.

Elevate security to a senior position. The chief security officer needs to report to the chief executive officer. If someone does not represent the security and risk-assessment capacity at the highest levels of management, a gaping hole exists within the organization. A breach at the facility will prompt shareholders to ask why the company did not take the prudent measures exercised by sophisticated firms committed to security.

Exercise the security plan. In addition to planning for emergency situations, companies must practice those procedures on a regular basis to ensure their effectiveness. Often, paper solutions present logistical difficulties when implemented. Firms need to communicate the details of emergency procedures to all employees and conduct ongoing drills to facilitate their smooth execution in the event of a crisis.

Two years after the deadliest terrorist attack in U.S. history, the nation remains unprepared for a future assault. The report published on the findings of the joint inquiry offers little optimism concerning the ability of the U.S. intelligence community to detect the new strike. Instead, this document sends a stark warning to the entire country: The enemy remains at large, planning the next attack.

For many the events of September 11, 2001, represent not a wake-up call, but a once-in-a-lifetime tragedy. The joint inquiry report reveals the foolishness of this complacent attitude. Al Qaeda has trained tens of thousands of soldiers to terrorize the United States. The U.S. government has captured or killed no more than 3,000; the rest lie in wait—a crafty enemy unlike any the nation has encountered.

Some organizations and individuals recognize the magnitude of this menace. Others jeopardize not only their own survival, but also the national security mission itself by focusing exclusively on the margin pressures of an economic recession. By failing to protect themselves—and thus their shareholders' interests—these companies will find any short-term, cost-cutting gains obliterated by the public backlash that would follow a successful assault against their facilities.



The Lipman Report Editors