

June 15, 2003

## June 15, 2003: Terrorist Threat

### Complacency and recession compound American vulnerability to terrorist attack

*Confusion reigns across much of the United States as individuals and organizations alike attempt to decipher the current global climate. Recent gains in the U.S. stock market, combined with the latest federal tax cut, give hope that the American economy may finally be recovering from recession, yet record unemployment rates indicate that financial woes could continue for some time. Meanwhile, decisive military victories in the Middle East reassure many Americans that the nation is indeed winning the war against terrorism. Supporting this belief is the lack of terrorist activity on U.S. soil since the tragic attacks of September 11, 2001. At the same time, continued attacks against U.S. soldiers reveal that the situation in the Middle East remains volatile. The result is fear and uncertainty in terms of safety and security.*

*Intelligence sources reveal that the terrorist threat to the United States and to Americans remains as great today as during the autumn of 2001. In some ways, the threat is even greater because the devastation of the assaults that toppled the World Trade Center in New York and collapsed a portion of the Pentagon raised the stakes: terrorist organizations now have a new benchmark against which to measure the results of their deadly operations. Compounding the situation is the recent recognition that the United States is not immune to the fatal attacks that routinely occur in other nations. Fear has become a new component of the American mindset.*

*This fear, however, can work against the terrorists. Remaining mindful of the ongoing threat, businesses and individuals can take proactive steps to thwart future assaults, thereby converting potentially paralyzing fear into a fearsome resolve.*

### Continued complacency

A study conducted for Guardsmark, LLC, by Penn, Schoen & Berland last March revealed a widespread complacency in corporate America, despite the fact that 96 percent of respondents believed that terrorism remains a serious threat. Of more than 200 security professionals and 600 members of the general public interviewed, clear majorities in both groups perceive that workplace security has become too loose and relaxed because no terrorist attacks have materialized in the United States since September 11, 2001. More than 50 percent of the American people

indicated that their companies were doing nothing to prepare for another terrorist strike.

Experts report that much of this complacency appears geographically related: organizations in the central regions of the country are markedly less concerned about security than those on the East and West Coasts. Companies in the Northeast have the greatest focus on security in general and terrorism in particular.

The overwhelming success of U.S. military campaigns in Afghanistan and Iraq further contributes to this false sense of security. The demonstrated supremacy of Western military forces has convinced many Americans that the United States is effectively winning President George W. Bush's declared war against terror. An endless stream of intelligence "chatter" and recent bombings in the Middle East, however, reveal that the war is far from over.

### Waiting to strike

For many Americans, the fact that no attacks have taken place in the United States since September 11, 2001, represents victory. Those familiar with al Qaeda and militant Islam understand that for each person being hunted or in custody, there may be hundreds of other terrorist sympathizers getting ready to strike. The ranks of these potential enemies to our way of life will not diminish, as long as economic and cultural chasms continue to divide our world.

Certainly, the country has made tremendous progress in weakening this terrorist organization. During the last 18 months, the United States has eliminated several key leaders, arrested 3,000 operatives around the globe and shut down 50 terrorist training camps in Afghanistan. Federal law enforcement authorities believe that interrogation of these operatives and subsequent investigation of leads have contributed to the lack of recent domestic attacks. One potential attack that surfaced after the capture of Khalid Sheik Mohammed involved the

(continued on next page)

---

## June 15, 2003: Terrorist Threat

### Complacency and recession compound American vulnerability to terrorist attack

(continued from preceding page)

Metrorail system in Washington, D.C. Other targets disclosed include the U.S. Capitol and the Israeli Embassy in Washington.

Last month's bombings in Riyadh and Casablanca serve as poignant reminders that al Qaeda is far from neutralized. The attacks, which left more than 70 dead, were followed by an exhortation by Osama bin Laden's top deputy, Ayman al-Zawahiri, for the faithful to execute additional strikes against Western embassies and businesses. This call to action was not idle, and Americans need to remember the example of the World Trade Center: al Qaeda began plotting the attack of September 11, 2001, on February 26, 1993, when the initial assault failed to bring down the twin towers.

#### Wide-reaching targets

While the specter of the next major attack continues to shadow the nation, the United States must address the threats facing a less conventional, but more dangerous, target: its infrastructure. Studies of homeland vulnerabilities have long identified significant weaknesses in the networks governing such critical sectors as transportation, utilities, banking and finance, water, emergency services, government services and telecommunications. To date, however, most security initiatives have focused on physical security—barriers, electronic systems, uniformed guards. Far too little progress has been made in developing an effective response to an infrastructure attack, which would include speedy restoration of the affected systems.

These critical sectors represent the nation's lifeblood. Failure either in part or whole of the financial or transportation networks, for instance, could produce pandemonium in the world markets—exactly the sort of global consequence desired by modern terrorists.

The food and agriculture industry represents a target to both terrorists and homegrown extremists.

One animal-rights group has threatened to introduce foot-and-mouth disease in the United States. The recent outbreak in the United Kingdom illustrated the devastating effects of such an event on markets both at home and abroad. In the event that an agricultural outbreak of this nature occurred, the United States would not be able to contain the disease or contamination because of inadequate public communication networks. According to a recent exercise, by the time the U.S. Department of Agriculture confirmed the first case of foot-and-mouth disease through cross-border contamination, the infection would likely have spread through more than half the country.

Unfortunately, the U.S. government alone cannot patch these vulnerabilities with legislation and resource allocation. The majority of the country's infrastructure rests in private hands, demanding extensive cooperation throughout private industry. Furthermore, the overwhelming scope of the problem demands untold billions in financial resources and will take years to implement, even if acted upon immediately. The current economic recession, as well as the prevailing complacency, makes such action unlikely in the foreseeable future.

#### Weapons of mass destruction

Various reports have emerged in the media that question whether the Bush administration had adequate evidence concerning Iraq's weapons of mass destruction (WMD) program to justify the attack against that nation. This debate contradicts years of intelligence indicating that Iraq did indeed have a substantial WMD program, including testimony from Iraqi scientists who participated in the effort. The fact that coalition forces have not yet found these weapons reinforces the reality that the recent war may not have succeeded in eradicating Iraq's WMD capability: those weapons may still be at large.

Additionally, stories continue to surface about al Qaeda and its quest to obtain WMDs. At the very least, the group is attempting to procure enough radioactive material to produce a radiological, or

“dirty,” bomb, which uses conventional explosives to disperse radiation over a wide area. Such a weapon would have a threefold effect: injuries and potential deaths from the initial explosion, the radioactive contamination of the strike zone, and rampant fear and panic over radiation sickness. The threat becomes more chilling given that no one doubts whether the terrorist organization would use a WMD: the events of September 11 clearly demonstrated that human life holds no value in al Qaeda’s jihad against the West.

One could argue that terrorist use of WMD is significantly greater in the post-September 11 world. The magnitude of those attacks forever altered Americans’ perspective. Last October, when terrorists killed more than 200 people at a Bali nightclub, the United States was horrified—but not necessarily terrified. The overall number of terrorist attacks has not decreased in the months since September 11, but most Americans do not attach much significance to them for two reasons: the casualties have been relatively low and the attacks have taken place in distant lands. These two factors have, for the most part, allowed many Americans to believe once again that terrorists would not dare strike them again at home.

At the same time, many of the men and women entrusted with protecting the nation are experiencing a very different reaction. Security directors in a wide spectrum of industries across the country worry greatly about the next domestic attack, and WMD often top their list as the most serious concern. For these individuals, September 11, 2001, demonstrated the need for protection against the unthinkable. Little can be done once an attack has been launched, but a solid security program can prevent an assault from happening in the first place. In the aftermath of any significant attack—regardless of whether it comes from terrorist or more conventional sources—the men and women responsible for safety and security recognize that the wrath of shareholders, customers and the general public will come down swiftly if investigation reveals that poor security contributed to the event.

### **Proactive preparations**

Security experts agree that a large-scale terrorist assault is not a question of “if,” but “when” and “where.” To protect themselves against this occurrence, organizations need to harden their defenses with concrete steps that will also help ensure business continuity in the face of a wide range of emergency events.

Many organizations have had some form of security plan or program that was instituted or considered for implementation following terrorist attacks: the 1979 Iran Embassy takeover, the bombing of the *USS Cole* or other tragedies. Whatever plans or programs may have been established or considered in response to terrorism and then put on the back burner need to be returned to the front burner immediately.

***Develop an intelligence network.*** Businesses need to develop information-sharing partnerships both within their industry and within their geographical region. Recognizing the need to protect proprietary information, companies should form alliances with other firms, as well as with government and non-profit organizations, for the overall aim of strengthening security. Such networks should communicate the various threats member facilities face throughout the world and the solutions they have implemented to mitigate these risks. Regional partnerships that unite organizations from different industries can offer a range of valuable perspectives, yielding greater insight than a network comprised of homogeneous businesses.

***Perform a thorough risk assessment of the facility.*** Every organization must review and analyze the types of risks that threaten their employees and facilities. Potential threats could arise from a variety of specific factors, including geographic location and industry issues, or from a range of general risks, like crime and workplace violence, that can occur anywhere. Enlisting professional services to conduct the

(continued on next page)

## June 15, 2003: Terrorist Threat

### Complacency and recession compound American vulnerability to terrorist attack

(continued from preceding page)

assessment will help ensure that the audit provides a comprehensive, unbiased analysis. Companies must recognize, however, that the effectiveness of security surveys lies in the implementation of security recommendations. Failing to correct weaknesses identified by the assessment could expose a business to liability.

**Build relationships with local, state and federal emergency responders.** Companies need to develop partnerships with these agencies before a crisis occurs. Private enterprises should alert local law enforcement of any suspicious activities or other irregularities they may encounter, thereby providing an early warning. Conversely, the more information that the fire, police and ambulance services have about a facility's layout and procedures before an incident, the more rapidly and effectively they can respond in an emergency. Cultivating such a relationship will also give an organization a realistic view of the assistance these agencies can provide, as well as their limitations, during a crisis. In the event of a wide-scale emergency, firms need to have the appropriate personnel and procedures in place to supplement public emergency response officials.

**Back up information technology (IT) resources in a distant offsite location.** The integral role of IT in everyday business processes requires continuous access to this vital information. In addition to performing regular system backups, administrators need to store copies of this data in a secure, offsite location, where they are available for quick retrieval. Larger companies should consider investing in a redundant system, maintained in a geographically distant facility, that can sustain business operations if the primary system shuts down. Several IT firms offer these total system backup services, in which they stand ready to switch an organization's operations to their systems as needed.

**Develop and communicate a comprehensive emergency response plan.** Companies of all

sizes need to create a detailed, written plan of procedures to address such issues as business continuity, employee evacuation and emergency communication, and public relations. The plan should assign tasks to specific individuals to handle any foreseeable crises that may occur. This program should also convey clear instructions on how to lock down and evacuate the premises, as well as how to communicate with employees, their families and the general public during and after an emergency situation. Businesses must disseminate the details of these plans to personnel on a regular basis and conduct drills to help ensure their effectiveness in an actual emergency.

*The Beirut Marine tragedy. The Libyan campaign against the West. The destruction of Pan Am Flight 103. The Khobar Towers bombing in Saudi Arabia. The bombing of the U.S.S. Cole. For more than two decades, adherents of militant Islam have wrought death and destruction around the globe in their war against Western civilization. The attacks of September 11, 2001, represented a new turn in this terrorist campaign: the first successful, catastrophic strike against the United States on its home territory. A new tactic has been launched in the terrorist campaign; the war has moved to a new level.*

*The nation must tread very carefully in the upcoming months. As the economy teeters toward potential recovery, organizations must continue to exercise heightened vigilance and address the ongoing terrorist threat. A successful attack on American soil at this stage could be the trigger that sends the global economy into a long-term spiral.*



The Lipman Report Editors