

August 15, 2003

Mission: Enhancing preparedness of America's private sector

Government emergency response capabilities are still inadequate

While the terrorist strikes of September 11, 2001, represent the apex of terrorist activities against the United States, they are but one example of several dozen attacks or attempted attacks targeting U.S. interests during the last quarter century. Even as the United States has committed significant resources to thwarting future terrorist threats, intelligence reports still suggest that additional plots continue to be developed and a future attack is likely. Indeed, the number of anti-American terrorists and their sympathizers around the world may now be greater than ever.

Still, many Americans do not perceive the terrorist threat as their problem. They may believe that the targets are a few symbolic buildings in New York or Washington, D.C., not a factory in Kansas or an office building in Florida. And even if the attack does occur, many people believe that the government is prepared with emergency response plans and adequate resources. Unfortunately, no one knows when or where terrorists will strike next, and the country's emergency response infrastructure is not adequately prepared in most localities. For America to be truly prepared, a partnership must exist among federal, state and local governments and the private sector. Each of these groups must do more, and no single group can achieve this goal alone. It is imperative that all management—particularly senior management—consider security a top priority within their organization, proactively assessing existing vulnerabilities and developing and exercising contingency plans. Their jobs, their brands and the enterprise value of their corporations are at stake.

Civilian soft targets likely

A recent Congressional report about the September 11, 2001, attack revealed that between 40,000 and 100,000 terrorists from 56 countries around the world received training in terrorist camps in Afghanistan on such topics as explosives, kidnapping and assault. The Federal Bureau of Investigation has suggested that only about 3,000 of these individuals have been apprehended to date. Included in the list of terrorists at large are 38 of the top 52 al Qaeda leaders, including Osama bin Laden and his top deputies. The conclusion is clear: too many potential terrorists—including “sleepers,” who integrate themselves into society

before being called to strike, probably in the United States—and terrorist sympathizers remain at large to feel that the country is safe from further attack.

The question that many in the intelligence communities ask therefore is not whether further terrorist attacks will be attempted in the United States, but rather when, where and how. These experts suggest that a wide array of targets could be pursued by terrorist organizations such as al Qaeda. Some believe that terrorists will once again focus on prominent sites, targeting such structures as the White House, the U.S. Capitol and other landmark buildings and bridges. These types of attacks would be designed to produce flashy media images of fallen American icons, which could be a morale boost for terrorist sympathizers in the Middle East and elsewhere.

Other experts, however, caution that the next attacks could strike at less prominent targets, perhaps even in smaller cities away from the Eastern seaboard. Such a terrorist strategy would aim to paralyze the U.S. economy—the engine of America's strength and the glue that holds the world order in place. Targets could include important infrastructure facilities, such as water treatment facilities, power plants or chemical plants, as well as a wide array of businesses in all sectors of the economy. Potential motivation for such attacks on “soft” targets would be to destabilize the American way of life by undermining the confidence of U.S. consumers and investors. For example, an attack on a water treatment facility could destroy an entire city or paralyze it for months. Similarly, even an attack on a shopping center, while not appearing to significantly disrupt the nation's infrastructure, could have a devastating impact as consumers lose confidence in the ability of retail establishments to provide a safe environment, which would in turn decrease consumer spending.

Furthermore, many members of the intelligence community are alarmed by the potential for attacks initiated by sympathizers of al Qaeda, Iraq or

(continued on next page)

Mission: Enhancing preparedness of America's private sector

Government emergency response capabilities are still inadequate

(continued from preceding page)

militant Islam, individuals who are not directly associated with terrorist organizations but who support their cause and methods. These individuals could react to public calls from terrorist leaders or to other terrorists' acts and strike at soft targets, which could be more vulnerable. Furthermore, sophisticated planning would not necessarily be required for an attack on a soft target to be successful. These types of threats are the most difficult to detect in advance and thus the hardest for the law enforcement and intelligence communities to prevent.

Government agencies unprepared

Despite the looming potential threat of terrorist attacks aimed at soft targets throughout the country, the various federal, state and local government agencies have not focused adequately on enhancing emergency response capabilities. The Independent Task Force on Emergency Responders, a mission of the Council on Foreign Relations, recently released its report "Emergency Responders: Drastically Underfunded, Dangerously Unprepared," detailing America's state of preparedness for such potential incidents. The report—a culmination of months of work by such well-known public policy figures as former Senator Warren Rudman and former National Security Council Special Adviser Richard Clarke—brought to light serious deficiencies in emergency preparedness, including the following:

- Only 10 percent of the fire departments in the United States have the personnel and equipment to respond to a building collapse;
- On average, fire departments across the country have only enough radios to equip half the firefighters on a shift, and breathing apparatuses for only one-third.
- Public health departments do not have basic equipment or expertise to deal with the aftermath of chemical or biological attack, and 75

percent of state laboratories already report being overwhelmed by too many testing requests;

- Emergency responders in most localities do not have the capability to determine what kind of hazardous materials were used in a suspected terrorist attack;
- Police departments do not have necessary equipment to protect themselves from weapons of mass destruction.

In many cases, government agencies have been unable to cut through the red tape of dealing with jurisdiction and re-organization issues following the establishment of the Department of Homeland Security to develop adequate emergency response plans. Lack of sufficient funding has been the primary obstacle: the authors of the report suggest that an additional \$100 billion should be spent on homeland security emergency preparedness initiatives in the next five years to close the preparedness gap for critical emergency response mechanisms. Until such funding is appropriated, the emergency preparedness initiatives will have to rely on limited funding from the Department of Homeland Security, as many states and localities are choosing not to pursue such programs because of their own budget deficit problems. The growing federal government deficit, combined with budgetary pressures from the military expenditures in Iraq, makes it uncertain whether additional federal funds will be released to bridge the gap in state and local spending on homeland security initiatives.

Private sector can do more

With so many things remaining to be done, so few resources and so little time, the government cannot be expected to tackle the entire task of preparing the country for emergency response to a terrorist attack. Although the potential for a terrorist attack continues, the recent economic downturn has prompted many organizations to consider cutting back their security expenses. A survey commissioned by the Conference Board revealed

that average corporate spending on security has increased by only 4 percent since the September 11, 2001, attack—after adjustment for inflation that means that in real terms companies are purchasing less security now than they did before September 11, 2001. These findings corroborate an earlier study commissioned by Guardsmark and conducted by Penn, Schoen & Berland Associates, which revealed that many security professionals and members of the general public felt that the companies they work for were complacent about security. In fact, 55 percent of the security professionals reported that their companies were not preparing backup facilities at other sites, and more than 40 percent of respondents indicated that their companies were not conducting emergency drills, backing up files at a remote site, creating more effective firewalls to prevent hacker attacks, or conducting tighter background screenings on potential new employees.

It should be acknowledged that even the most sophisticated security system cannot ever offer a full guarantee of preventing a disaster from happening. Terrorist and criminal groups are always thinking of new and better ways of striking at their targets. However, a sound security plan can help minimize the impact if a disaster were to occur by coordinating the response to the incident—whether that involves evacuation of personnel, activation of a crisis management team or implementation of a business continuity plan.

When thinking about long-term security, organizations should consider that the terrorist threat represents just one of a number of risks they face; other risks can include workplace violence, theft, sabotage, corporate espionage and ordinary street crime.

A security disaster can happen at any time and anywhere, with potentially devastating results to the company's employees, customers and public reputation. Years of building up brand equity and enterprise value can be destroyed with a single incident. The following five recommendations

present simple, yet effective, measures to build or enhance a corporate security program:

Foster a collective corporate responsibility for security. Security is an issue of utmost importance to companies because its application can mean the difference between life and death for its employees, customers and ultimately for the company itself. Because of the critical nature of this responsibility, organizations should have a corporate governance model where there is a collective responsibility for security at the “C” level—among the Chief Executive Officer, Chief Financial Officer, Chief Security Officer, and the heads of human resources, information technology and other key departments. Each of those involved in security decisions should know what the CEO is most worried about. The person responsible for security should be elevated to a “C” level security position and should have the backing of all top-level management to enable him or her to make and implement decisions that are in the best interest of the company as a whole. Security is a serious concern; there is no room for company politics or finger-pointing. Everyone within the organization must work together and share responsibility for this critical function.

Implement an overall risk management strategy. Many corporate boards and C-level executives have a risk management strategy for business aspects other than security: action by competitors, the financial markets and insurance—which companies now pay more for even when resisting additional expenditures on security. Each organization should have a risk management strategy for security that quantifies how much it will cost to protect against an incident occurring, what is the likelihood of such an occurrence and how much more it could cost if an event takes place. Consider the costs beyond what insurance could reimburse, such as liability expenses, damaged brand equity and loss of consumer confidence. Knowledge of these facts can help business lead-

(continued on next page)

Mission: Enhancing preparedness of America's private sector

Government emergency response capabilities are still inadequate

(continued from preceding page)

ers make decisions about security in a rational and informed manner. To some managers, additional security allocations may appear staggering, but the expense might be miniscule compared to the potential costs if the organization does not have adequate security and a terrorist strike or other disaster hits.

Perform an independent vulnerability assessment.

This serves as a critical first step in any effective security program. It should not be conducted internally, but by a professional security team. Such an approach will ensure sufficient expertise and give a fresh perspective while avoiding potential conflicts of interest. First, identify the company's critical operations, loss of which could shut down business. Next, identify the range of threats facing the facility and prioritize them based on their potential for occurring and their potential consequences. The vulnerability assessment should focus on internal and external vulnerabilities and give managers some idea about the potential implications of each vulnerability. This will allow those responsible for the security function to prioritize areas of concern.

Take a comprehensive approach to security.

Looking at a security program only in terms of security officers, access control technologies or security cameras will not work. All of the existing vulnerabilities must be evaluated, and each vulnerability has to be addressed by a proactive solution. Do not just think of the organization's core daily processes. Think also about the people, property and procedures. What is critical to the operation of the organization? Where are the facilities? Who are the employees? Who are the customers? Who are the vendors? Who are the vendors' employees?

Exercise to prepare for an emergency. Each organization should think about and plan for emergency contingencies. This type of planning involves designation of crisis management teams, development of emergency response scenarios

and creation of business continuity plans.

Companies can conduct tabletop exercises simulating different types of disasters to go through the mental steps management would take in different settings based on potential emergency scenarios. On September 11, 2001, Americans had no idea that a terrorist attack was going to destroy the World Trade Center. Once it did, the country grounded airplanes, launched fighter planes, and closed borders and ports within an hour.

Government agencies were able to go through a checklist of things to do because they had practiced it twice a year, every year with all of the agencies involved, so each one had plans in place for a potential emergency scenario. Companies in the private sector should be just as prepared.

There are 24 million businesses in the United States, each one of them a potential target for a terrorist group or a terrorist sympathizer. Protecting these businesses are just 800,000 law enforcement officers—that is one law enforcement officer for every 30 businesses—with the vast majority of these officers directed at protecting citizens, not just businesses, and fighting ordinary street crime, not terrorism.

If the private sector does not take steps to protect its own facilities, chances are that no one else will—not the federal government, not the state or local government. Employees cannot do it alone. Ultimately, the responsibility for security rests with the management of each facility and of the company as a whole. By taking a proactive, comprehensive approach to security and establishing a collective responsibility for security within top management echelons, the corporate community can play a vital role in making workplaces in the United States safer than they are today.



The Lipman Report Editors