

Directors & Boards

THOUGHT LEADERSHIP IN GOVERNANCE SINCE 1976

THIRD QUARTER 2005

How secure is your building?

By **Bruce T. Kennedy**

The terrorist attacks of Sept. 11, 2001, were perhaps the ultimate example of failed building security. But there was nothing the owners, managers, and tenants of the World Trade Center could have done to prevent terrorists from flying jumbo jets into those doomed towers that terrible day.

Fortunately, there is much that owners, managers, and tenants can do — and may soon be required to do — to reduce their exposure to less apocalyptic but far more likely incidents at buildings they own, manage, or occupy.

As the 9/11 Commission's Final Report notes, the private sector controls 85 percent of the nation's critical infrastructure, so unless terrorists specifically target a government facility, the first "first responders" are likely to be civilians. Accordingly, the report continues, private-sector preparedness for rescue, restart, and recovery after acts of terrorism should include (1) an evacuation plan, (2) adequate communications capabilities, and (3) a plan for continuity of operations.

After 9/11, the federal government — and specifically the Department of Homeland Security — focused initially (and properly) on protecting government installations and such critical public sites as airports, hospitals, and schools. More recently, federal officials have begun to reach out to the private sector to coordinate contingency planning. One outcome: The American National Standards Institute (ANSI) has developed — and the 9/11 Commission has endorsed — a "National Standard for Preparedness" for the private sector (more commonly known as NFPA 1600).

The Commission is also encouraging the insurance and credit-rating industries "to look closely at a company's compliance with the ANSI standard in assessing its insurability and

creditworthiness." Once that happens, companies failing to comply with the ANSI standard may not only face increased risk to their workers and facilities, but also expose the company's shareholders and directors to the financial fallout from that failure.

What can companies and their boards do to protect the buildings that house their employees, operations, customer records, and other vital assets? A complete answer is beyond the scope of this article. But for openers, they should consider the following.

In one case we know of, an executive's '24/7' bodyguards weren't required to follow him into his own building, so they weren't there to protect him from the disgruntled worker who held him hostage for three hours in his own elevator.

Executive protection is needed on both sides of the company's front door. Even after an executive is "safely" inside, he or she may be exposed to attack by a disgruntled employee, be subject to another tenant's crisis, or suffer a workplace disruption arising from a bioterrorism event around the corner. (In one case we know of, an executive's "24/7" bodyguards weren't required to follow him into his own building, so they weren't there to protect him from the disgruntled worker who held him hostage for three hours in his own elevator.)

Access to both a company's building and its offices within that building must be strictly limited and controlled at all times. That means, at a minimum, a photo ID, preferably government-issued, to get past the building lobby and into the elevator bay. It means a building guard

phoning upstairs to confirm that a visitor is expected. Cumbersome, time-consuming, and annoying to the bona fide visitor, perhaps, but it's the best way we know to keep the bad guys out and the good guys safe from harm.

Boards should require management to arrange top-to-bottom reviews of their security preparedness by qualified, independent experts, who should assess such key areas as employee and visitor admission, loading dock access, messenger center protocols, security personnel and training, liaison with local public safety authorities, the presence and adequacy of closed-circuit TV (CCTV) surveillance equipment, the protection of mechanical rooms and utility closets, and emergency procedures and policies.

Finally, the adequacy of the emergency preparedness should be reviewed on an audited, annual basis to ensure continuing compliance.

Building security can take many forms. Most of these can (and should) be transparent to workers and visitors alike, but all can meaningfully enhance the security and safety of the building as well as the workers and other assets it contains. A qualified expert, who performs a thorough building security analysis and provides specific electronic, behavioral, and other recommendations, can help ensure that the building a company calls home is as safe as possible from all but the most catastrophic and unpreventable disasters and attacks.

***Bruce Kennedy** heads the James Mintz Group's security consulting team, and advises clients on building and computer security, emergency preparedness, theft of intellectual property, and executive protection. He is respected in the field as a security and anti-terrorism expert with more than 40 years of technical experience, including 20 years with the NYPD. Bruce can be reached at bkennedy@mintzgroup.com.*

Reprinted from Directors & Boards® Third Quarter 2005

© MLR Holdings LLC • 1845 Walnut Street, Suite 900 • Philadelphia, PA 19103

(215) 567-3200 • www.directorsandboards.com