Corporate counterterrorism presents both complex challenges and surprising opportunities, but too many companies still don't take the threat seriously enough. By Michael J. McDermott

Safety FIRST

Illustrations by Dan Page

Suddenly, the world has become a much more dangerous place to do business. Top executives on both sides of the Atlantic have no choice but to face the reality of a post-9/11 — and now, since the Madrid train bombings, post-3/11 — world. Terrorism, whatever its causes and whoever its perpetrators, has raised the stakes considerably in the corporate security game.

To date, however, the corporate response to terrorism's growing threat has been more "evolutionary" than "revolutionary," according to Tom Cavanagh, senior research associate and the in-house security expert at The Conference Board, a not-for-profit research and business organization with more than two thousand corporate members in sixty-six nations. After September 11, he notes, many observers expected companies to align such functions as physical protection, risk management, and IT security under a chief security officer. Movement in that direction, however, has been slow.

ST

The median increase in security spending was just four percent in the year after September 11, according to a Conference Board report released in July 2003. More dramatic increases in security spending have been rare and concentrated in a handful of industries. Just seven percent of companies surveyed for the report — which was sponsored by ASIS International, an organization of security professionals with more than thirty-three thousand members worldwide — increased security spending by fifty percent or more.

UNMET SECURITY NEEDS

Clearly, most multinational corporations still have unmet security needs, especially in the "strategic alignment area" identified in the Conference Board report, and that should lead to new business opportunities for some companies. Spending to date has been overly focused on "guns, gates, and guards," says Jake Stratton, director of research at the London office of Control Risks Group. "That is a blunt and ineffective solution to a problem that is more complex than it appears," he says. "What is needed is an increase in strategic thinking in addressing this issue."

Across the board, private-sector security spending has fallen short of expectations. A November 2002 report from the Federal Reserve Bank of New York pegged expenditures among U.S. companies in 2001 at $32.8 billion. The report noted that if annual spending doubled to reflect the new threat environment, an additional $7.8 billion would have gone for capital equipment and $25 billion for personnel in 2002. Analysts at the Brookings Institution and other research organizations believe overall spending fell far short of doubling in 2002, however, and more recent data indicate little change in that pattern. In a survey for its 2004 Security Industry Forecast, for example, *Security Industry* magazine found a mix of growth and cutbacks, with some security professionals saying their biggest operational concern is managing budget cuts ordered by their firms.

Statistically, the most serious threats to companies in both the United Kingdom and the United States remain non-terrorist-related. Large companies are much more likely to be affected by theft, fraud, unauthorized or malicious leaks of information, fake résumés, or industrial espionage than by terrorist action, points out Major General Walter Courage (Ret.), director of business development with The Risk Advisory Group Ltd. in London.

Jeffrey Klink, chairman and president of New York-based Klink & Co., agrees. "Planning for and responding to crises, protection of executives and other personnel, and protection of facilities and assets, including intellectual property, are some of the major issues that need to be addressed," he says. Because most security breaches are the result of internal rather than external forces, companies need to focus on knowing their own employees. "Too much money is being spent on high-tech gadgets to keep people out of buildings, and too little money is being spent on other crisis management tools," he adds.

That said, all the security experts contacted by *UK&USA* for this article agree that the threat of terrorism is a very real security issue for companies in both countries, and one that cannot be overlooked. "For companies doing business in the main commercial hubs of these countries, terrorism has to be near the top of the agenda," notes Stratton.

Dan Mead, the London-based director of operations in the security practice at Kroll Inc., counsels companies doing business in the United States and the United Kingdom to take an objective view of the exposure that their business, facilities, and employees face from terrorist threats. "The potential threat could be as a result of a direct relationship with U.S.-U.K. activities in Afghanistan or Iraq, or coincidental because of address," he observes. "Companies also need to be sensitive to their employees' perceived security concerns — for example, commuting on trains, tubes, and the like."

GEOGRAPHY INFLUENCES PERCEPTIONS

Attitudes toward the security risk posed by terrorist threats have differed from one side of the Atlantic to the other, suggests Crispin Black, a director of Janusian, the risk management subsidiary of Risk Advisory Group. "Although most Europeans watched the unfolding events of 9/11 on television and sympathized strongly with the suffering they saw, the events always seemed distant to many of them," says Black.

That was evident, Black says, in the reaction of many Europeans to the aggressive security strategy of the United States following the attacks on the World Trade Center and the Pentagon. The seeds of change in that attitude may have been planted in the tragic train bombings in Madrid on March 11 of this year, an event that pundits almost immediately began referring to as "Europe's 9/11."

"Madrid will also have an effect on the perception of the security challenges that companies face," proposes Courage, who believes the train bombings may well serve as a wake-up call for those who are still only in the very early stages of putting together a security strategy. "A terrorist attack may remain a low-probability event for an individual company," he allows. "But should a firm get caught up in a terrorist attack and have few physical or procedural security measures in place, not only will it suffer higher casualties, it will also suffer highly adverse reputational effects."

It is inevitable that the attacks will negatively alter corporate perceptions of risk in Western Europe, Stratton notes. "They demonstrate that for all the rhetoric about being on guard against terrorism, European cities remain vulnerable to simple yet devastating attacks," he says.

Although specific threats to corporate objectives might differ from those targeting the public at large, there is no doubt that there is significant overlap in the main areas of concern for both the private and public sectors. Accordingly, private industry groups and individual companies are working with the appropriate government agencies in both the U.S. and the U.K. to address security issues of common concern.

ADVICE FROM THE EXPERTS

UK&USA asked experts at some of the world's top security firms to put together a list of critical priorities for corporate decision makers. Here's what they had to offer.

1. **Adopt a strategic approach to security.** Start with a thorough audit of risk exposure that includes facilities, business processes, and employees. Use the results to craft a proportionate mitigation strategy.

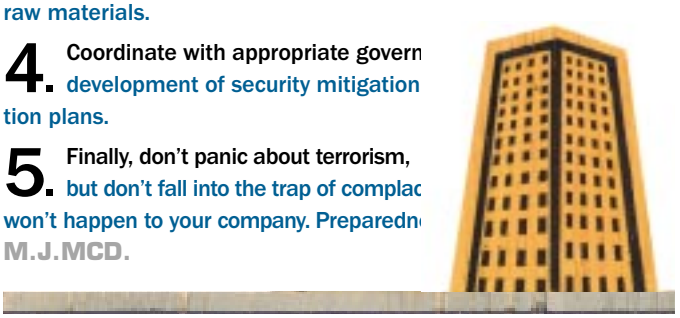
2. **Focus more attention on human resources considerations.** All employees should be trained in security awareness and crisis response, and a simplified system for reporting suspicious situations should be put in place. The ultimate responsibility for all security matters worldwide, including the protection of company executives at home and when traveling, should rest with a qualified chief security officer.

3. **Develop and practice a business continuation contingency plan for various scenarios** that establishes alternatives for resources such as housing, energy, communications, and raw materials.

4. **Coordinate with appropriate govern** development of security mitigation tion plans.

5. **Finally, don't panic about terrorism,** but don't fall into the trap of complac won't happen to your company. Preparedn

M.J.MCD.



COUNTERTERRORISM'S OPPORTUNITIES

Politics is politics, but business is business. As is the case with just about any situation that might arise, there are potential upsides related to meeting security challenges for those companies that choose to look for them. "There are always business opportunities in any crisis," Courage says. "For instance, when a company decides to put its security policy in good order, very often it can gain a better insight into the true, core nature of its business and the value of its employees. The security process acts as a spur to hard thinking and good corporate governance."

Organizations that make the effort to implement appropriate security measures before a crisis occurs can boost their level of protection from potentially ruinous legal costs and damage to their reputation further down the line, Mead says. Klink points to greater stability and the continued ability to deliver products and services in the wake of a crisis; protection of personnel and assets; and confidence in the business's ability to flourish in an age of terror and uncertainty as among the most valuable returns on investments in security planning and implementation. Both men see security emerging as a competitive advantage. "That is especially true if others in an industry are seen as fragile and vulnerable," Klink says.

The security industry itself, of course, is in an obvious position to benefit from stepped-up activity on the corporate front, with demand likely to increase for both consulting services and the provision of end-to-end in-house security operations. One of the challenges those in the industry face is getting clients to see enhanced security as something that belongs on the asset side of a company's ledger rather than on the debit side.

"While it is difficult to measure the value of rigorous security within a company, and therefore to see it as a positive contributor to the business rather than an overhead, I think the intangible value is growing strongly," Stratton says. "Businesses and their individual employees need confidence if they are to operate to their full potential, and the evolution of thorough and progressive security programs is a key element in building and sustaining that confidence throughout an organization."

For companies in both the U.K. and the U.S., facing the reality of increased security threats is an issue that can no longer be avoided. The only choice that remains is how it will be done. ■