

Homeland Security – Legal Service Providers

Homeland Security: Assessing, Mitigating And Responding To Security Risks

The Editor interviews **Russ Owens**, Senior Managing Director, Citigate Global Intelligence and Security.

Editor: What was the business community's response to the call for heightened security following the events of 9/11?

Owens: The immediate reaction of many companies to the events of 9/11 was to think that something different needed to be done right away, and they looked for a quick fix. As time passed, companies took more measured approaches. One positive result was the recognition by many companies of the need for a high-level security professional as a part of their senior management team. Most companies placed a reemphasis on their security organization and/or created such an entity within their business, enhancing the responsibility, stature and authority of the function. Another was to recognize the continual need to ask the question "are we doing what we need to do to protect the assets of our business?"

Editor: Where can a company begin to address its security concerns?

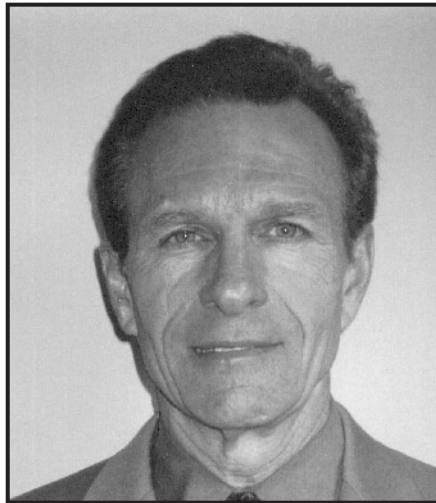
Owens: Senior management should be asking several key questions. What assets need protection? Why is protecting these assets important? Do we have the right mitigation strategies in place to prevent, reduce and deter the risks that threaten our assets? Are we in the position, if an incident occurs, to respond, recover and move on with our business?

Addressing these questions begins with a threat assessment. Before undertaking it, senior management needs to understand the need for the threat assessment. Commitment to the assessment and its implementation must be top down because a threat assessment is only effective if it takes into account all aspects of the company's business – its governance structure, employees, products, supply chain and marketing, distribution and sales channels.

Editor: What risks should be considered in a threat assessment?

Owens: Since 9/11, we have been preoccupied with terrorist activities and extremism. However, in addition to those concerns, there are a number of additional factors that need to be considered when identifying the potential threats to a business. International and domestic crime needs to be considered, and cultural considerations must be taken into account. Are there any reasons for threats and acts of violence directed at the people or property of the organization? Are the company's facilities located in areas of street crime or political or social unrest? Is there any exposure related to sabotage or product contamination? Another source of threats I call "product diversion," which can seriously harm key business objectives.

Exposure can include the risk of theft or loss of intellectual property, as well as physical assets. Therefore, any threat assessment must include exposures to



Russ Owens

computing and communications facilities, as well as to the company's physical plant and personnel. In addition to man-made harm, threats can result from natural disasters or consist of any combination or man-made and natural causes.

Editor: In what context should a threat assessment be conducted?

Owens: The most critical element is understanding the company's operations. What products and services does it offer? Is the company in research and development, manufacturing, marketing, consumer retail, entertainment, transportation or other industry? Who are its competitors and how intense is the competition? Who are its employees and what are their cultural perspectives, skill sets and work habits? Where are the company's offices, plants and personnel located? Are many company personnel assigned in foreign countries or regularly in travel status? Is the company dependent on its shipping and sales agents to keep its products and services moving through the marketplace?

A company also will want to ask a series of questions to get a better understanding of the inherent nature of the risks to which it is exposed. For example, is the company well known nationally or internationally? Is its logo or product line widely recognized? Is the company a symbol of American technology? Is it tied into government related or military operations? Are key personnel likely targets of kidnapping or other personal harm? Even if the company is not a likely target of sabotage or other harmful activity, is it located near a facility or another company at a higher risk level?

Another set of questions should assess the extent of harm that would be caused by the potential threats. That is, would the threat destroy or cripple a mission critical part of the company's operation? Would it shut down production or delivery? Would it result in a health hazard of one form or another to employees, visitors, subcontractors or customers? Could it result in significant loss of revenue for the business, customer loyalty or significant litigation? Could the media coverage be worse than the incident itself?

A full operational study should be done to answer these and other questions

relevant to the industries and countries in which the company operates. This provides a meaningful context for the threat assessment.

Editor: What are the principal elements of an effective risk mitigation strategy?

Owens: Once an operational study is completed, then mitigation strategies should be assessed to ensure that the company has the right resources in place to prevent, reduce and deter the threats identified as likely to occur. The mitigation strategies must be compatible with the company's culture so that they can be implemented practically and sensibly.

Mitigation strategies are often called Base Line Security. They usually cover such areas as physical security (protection of facilities), threat management (protection against violence against people or property), emergency planning and travel advisory programs.

The mitigation strategies should take into account the company's supply and sales chain. For example, a company may look at its own operations and see that it is in good shape. A supplier critical to its operations, however, may not have the same emphasis on security requirements. If the supplier does not safeguard its asset that will become part of the company's product line, it can shut the company down and have a major impact on the company's ability to deliver product. To mitigate such a risk, the mitigation strategy could include drafting and negotiating security requirements into its procurement contracts with its key suppliers.

Editor: What are the characteristics of a good program for responding to security risks?

Owens: From a public relations and media standpoint, a company cannot afford to have hostile publicity about any incident. Response to the incident needs to be well managed, and the company needs to demonstrate that it has recovered and moved on.

The lynchpin to a good response program is an effective Crisis Management Team. The team usually consists of senior management, general counsel, director of security/chief security officer, human resource executives, financial experts and media relations specialists. The team should be staffed with support personnel and meet periodically. The team's functions should include oversight of the company's security related policies, procedures and standards. These should be revised from time to time based on updated threat assessments. The team should receive reports from the "owners" of security processes. It should also provide oversight of the company's response to incidents when they occur.

It is generally considered to be a good practice for the Crisis Management Team to conduct a full-blown tabletop exercise on an annual basis. The exercise should be based on the most likely type of incident that the company is likely to

experience. The team's undivided attention is needed, away from cell phones and e-mails, to run through the scenario with different inputs throughout the exercise. As the hypothetical factors change, the team responds. The lessons learned should be fed back into updating the company's threat assessment, mitigation strategies and response program to keep them current.

Editor: How can corporate counsel help their companies to ensure that their response to the events of 9/11 is not to end up with only a document that identifies risks and solutions, but instead have an effective security program that is actually implemented?

Owens: One way is to bridge new solutions with what is happening in the business already. Policies, procedures and practices that are already working can be kept in place and others modified, updated, amended or totally replaced depending on the risks that have been identified. You need a set of step-by-step capabilities that can be implemented based on the company's culture. For example, procedures can enable personnel to say, "This particular phone call that came in relates to this type of threat, which based on past experience in prior assessments is or is not likely to be a hoax."

Editor: How can a company benchmark whether it is taking reasonably prudent steps in assessing, mitigating and responding to security risks?

Owens: There are a number of things that a company can do. First, the company should review its own history of incidents and ability to respond to them. In assessing the current situation, the company may find an excellent source of information in what its expatriots and indigenous personnel are telling it about local conditions.

Another step is to discuss with peers the problems they are facing, their losses and what programs have worked for them and what did not. The type of peers chosen may vary based on industry, geographic location or other variables relevant to the security risks that the company faces.

The company should also consider contacting government agencies to help with risk assessments, mitigation strategies and response programs. They can help assess the political climates in foreign countries, crime trends in particular geographic locations, and strength of law enforcement actions in various jurisdictions.

Companies that engage a consultant to initiate a comprehensive risk/threat analysis and operations study are fulfilling their fiduciary responsibility to their stockholders, board and employees by ensuring the assets of the business are appropriately protected.

If you have questions for Mr. Owens, you may contact him at (404) 431-5413.