JOURNAL OF COMMERCE, 23 May 2005

Risk consultants aren't all alike

J. MICHAEL BARRETT

Risk is calculated as a function of two primary factors: the likelihood of an event taking place and the severity of such event should it occur. That means that measures affecting either the likelihood of being targeted or the success of an attack are equally important in risk reduction. Because relative security values can be measured, analysts, investors and insurance firms also will choose to reward those companies that implement best practices, meaning security improvements help a firm's bottom line, as well as its survivability.

While cost is often the major determinant in selecting risk-mitigation consultants, understanding what you are looking for is the first step. Do you need a fully documented audit of total security business practices, a more cursory and primarily internal employee survey or an examination of physical and other vulnerabilities an enemy might seek to exploit? Fortunately, the risk-assessment industry is divided into three fairly distinct models: traditional, large auditing and consulting firms; other firms that use automated tools to perform systems processes surveys and make rough estimates of risk values; and firms composed of former law enforcement, military or terrorism analysts who offer rapid assessments based primarily on intuition and experience in understanding how adversaries exploit existing vulnerabilities.

The first group, marked by such marquee industry players as BearingPoint and Deloitte, is strongest in terms of business practice realignment and in-depth analysis of processes that affect overall security. They typically provide well-educated business analysts or very bright generalists who have learned security as an "additional category," as opposed to from deep personal experience, and can often spend up to a year on site, conducting large assessments.

The typical methodology for any business concern is to engage the clients and conduct interviews and assessments in-person to reveal inefficiencies and failings in current practices, with this model extended to security. This approach yields opportunities for improvement and internal reconfiguring, and is most applicable to those companies looking to aggressively restructure and realign their business processes as they relate to security.

The second group generally is characterized by individuals and smaller firms aided by the use of software tools, with each firm usually focusing on a specific industry. These audits are focused on where internal employees see potential problems arising, based on current company practices and standards. These analysts typically automate the survey process, which can cut the total product cost of their services dramatically by cutting on-site assessment time by as much as two-thirds.

This results in a less comprehensive but more affordable means of assessing one's basic needs. You may not be getting a highly trained security specialist, but that is not the focus; the focus is on creating surveys so that internal parties can report back on compliance with existing policies and procedures, how secure employees feel, and assessing any widely known vulnerabilities. This is the best approach for a firm that is certain it faces relatively low risk, does not wish to invest in the full audit model described above, and is primarily focused on surveying current practices.

The third type of firm provides the most comprehensive and specialized risk assessment specifically in terms of security, especially with regard to terrorism or other nontraditional threats. These companies are almost all staffed by former military members or law-enforcement agents who have deep and specialized experience and expertise in assessing security, both as the aggressor looking for holes to exploit and as the team assigned to protect a certain area. Their pricing is usually less expensive than the full-auditor approach in the first category, and comparable to the second.

Typically, their interviews about current practices will be less in-depth, opting instead to conduct exercises and simulations to test response times and procedures. They also will focus on the client's threats, vulnerabilities and security posture, drawing on experience to determine what additional safeguards would best cover the most likely, relevant and significant threats. These audits are the right choice for clients who are focused on defeating significant threats and want to improve their security posture by taking a hard, critical look at existing gaps in physical and procedural mitigation measures.

In the end, firms representing each of these three categories can provide a quality product. The answer of which firm to select lies in knowing which problem you want to solve and what goals you need to achieve. When it comes to risk mitigation, an educated consumer truly is the best customer.

J. Michael Barrett is vice president of Red Cell Associates, a consulting firm specializing in preparedness for terrorism and disasters. He can be contacted at (410) 224-7039 or at mbarrett@redcellassociates.com.