

SECURITY DIRECTOR

THE BUSINESS NEWSPAPER FOR SECURITY DIRECTORS

NEWS

www.securitydirectornews.com

marketwatch: **risk assessment**

SECURITY DIRECTOR NEWS

19

Risk assessment is foundation of a strong security plan

Security consultants and integrators can both offer an objective view of an organization's physical security needs

By JOANNE FRIEDRICK

Whether it's developing the big picture or reacting to a specific event, a risk assessment serves as the foundation upon which an organization builds its physical security plan as well as its policies and procedures.

Security directors have their choice of sources for these assessments, though typically the job falls to consultants or systems integrators.

When Dick Sproul was launching the first phase of a security project for the Taunton Municipal Lighting Plant in Taunton, Mass., the principal special projects engineer said he hired a consultant to perform a vulnerability assessment.

The assessment and recommendations were followed up with plans and specifications for an integrated security system.

While security consultants are reluctant to denigrate the services offered by an integrator, most are quick to point out that a consultant must offer an objective view, acting in the best interest of the client, not a vendor.

"There are multiple approaches and methodologies used to conduct risk and vulnerability assessments," said Dan O'Neill, president and chief executive officer of Applied Risk Management. Methodologies created by Sandia National Labs, FEMA, TSA and others, he said, "are available to consultants, integrators and in-house personnel. The scope of the project and assets being assessed typically drives methodology selection," he added.

But when it comes to which entity is selected to conduct the risk assessment, O'Neill said the consultant "is truly manufacturer and vendor agnostic. When a systems integrator conducts an assessment there is always the 'perception of bias,'" he said. "Even if the recommendations are in the best interest of the client, objectivity will always be in question."

"You have to be clear your recommendations are in the best interest of the company," said Harvey Schiller, chairman of GlobalOptions Group. "You have to be completely transparent."

OBJECTIVE VIEW

Jay Vaitkus, product and market manager for Stanley Security Solutions, which offers risk assessment via its integration services, said Stanley is also product agnostic. "We'll supply different lines of cameras and access control," he said. Vaitkus added that what an integrator can bring to the assessment process is knowledge of how products work together, as well as the ability to install and service a system and even finance the package.

Integrators, he said, often work with a consultant, especially on larger

projects. "Security consultants are usually looking for an integrator as a partner," said Vaitkus. "Some of the larger projects need a team."

At WFI Enterprise Services Division, President Desmond Wheatley said the integrator sometimes takes on the role of consultant. But in addition, he said, they work with clients and consultants, "who are independent of the integrator or the vendor."

As a consultant, Ira Somerson of Loss Management Consultants Inc.,

Tom Clayton of Clayton Consultants.

As a company that specializes in international security consulting, Clayton said those conducting risk assessments must have intimate knowledge of the countries in which they work.

A company in Latin America, he said, faces risks from kidnapping, but also from volcanoes. In areas such as Afghanistan and Turkey, earthquakes, not just terrorists, are a part of the equation.

"We in the security business tend to get encapsulated in our own cocoon," explained Clayton, "but the client has to have someone who looks at the entire scope of risk."

While Clayton emphasized the need to have a broad risk assessment, he said some clients do want just a physical security assessment.

If an enhancement to a security system needs to take place, he said, "we will suggest what needs to be done, but leave it up to them to do it." He said security directors often have their own preferred suppliers and it is up to the client and the integrator to determine what specific products to install.

REACTIVE MEASURES

Vaitkus of Stanley Security agreed that customers are often asking for an assessment of a specific location based on a specific event that has taken place. "The security business is very reactive, rarely proactive," he said.

"If a customer has an experience (such as an incident in a parking lot), they have to deal with that," he said. "But sometimes we can convince them

that they need to look at the whole picture."

Somerson said he rarely keeps a client beyond the initial consultation. Rather, he said, as part of the risk assessment, he establishes company focus groups that are charged with revisiting the plan on a yearly basis.

CASE BY CASE

Helping make the case for risk assessment is the increasing participation of senior management in the security process, experts said.

Schiller of GlobalOptions Group said "things are moving toward the top tiers of management." Companies, he said, "want to act with confidence no matter what the challenge will be," so senior managers are more involved.

Because of the awareness at the highest levels within an organization, Schiller said security directors shouldn't rely on handling the risk evaluation themselves. "The presentation has to resonate with senior management," he said.

Vaitkus said both the chief information officer and the chief financial officer are getting involved in risk assessment and the solutions offered. "We see more CIOs involved in security design because they (security) use the network," he said. Likewise, the CFO is interested "because they want to know what it costs and the return on investment."

Even if a risk manager initiated the assessment, Clayton said he gets the security director involved in the project as well because the crisis management or security plan is vital to the response to the assessment. "The first thing they should have is a policy," he said, followed by the procedures and systems to put into effect. **SDN**



"You have to be clear your recommendations are in the best interest of the company. You have to be completely transparent."

—Harvey Schiller,
chairman,
GlobalOptions Group

said while he's not selling any products, he does try to facilitate the buying process for his client. "The integrator is essentially a marketer," said Somerson. "You should have a risk assessment before you call in an integrator."

He said having a consultant as a liaison between the client and the integrator can be advantageous for both groups. The company will save money by not overbuying, he said, and he, in turn, helps the integrator make a case for what really needs to be included in a security system.

"If I go do the assessment and there needs to be a technology aspect to it," said Somerson, "I bring in an integrator or technology consultant." He also works in tandem with the IT department for risk assessment, or brings in a specialist in IT if a company has a high reliance on IT.

"The one who scares me is the consultant who tries to be all things to all people," he said.

FACTORING IT IN

Robert Schultheiss, principal consultant, Risk Decisions, said risk assessment is moving toward an integrated approach, including information technology security along with physical security.

"Information systems security used to be more about keeping the system up and running and now it's switching to what is on the system," he said. Like Somerson, Schultheiss said when he deals with information security, he brings in a consultant with risk assessment expertise in that area.

GlobalOption's Schiller agreed that IT has become a factor in risk assessment. "It would be silly to do an assessment that excludes IT," he said. A company's proprietary information is all part of its vulnerability factor.

Local and specific knowledge is also important to a risk assessment, said