

December 2003

**Key To The Future  
Security Opens Doors To New Business**

by Carolyn Heinze

The NSCA (National Systems Contractors Association) will have company next March at the organization's annual conference and trade show. During the event, which takes place in Las Vegas from March 19-21, the PSA Security Network will host a special product showcase focused on security and life safety technologies, in addition to overseeing the security/life safety education track. The alliance brings NSCA and PSA members under one roof: PSA will be offering a number of seminars for systems integrators, in addition to hosting sessions exclusively for those belonging to PSA.

This development reaffirms what many have known for a while—security is no longer an entity operating separately from the rest of the technologies which fall under the increasingly general category known as "systems integration."

"Today's building owner or facility manager doesn't like the concept of having to have so many redundant cabling schemes and wiring configurations within their buildings," said Chuck Wilson, executive director of the NSCA. "They want to see an intelligent building network infrastructure which incorporates all the different electronic system applications. They want to be able to manage that, see how they can expand it, and minimize the duplication of cabling."

This trend towards an "all-in-one" package presents new growth opportunities to systems integrators who have not previously touched the security segment of the installation market. "There is a real opportunity to be involved, because there is going to be a continued convergence of those types of systems—the obvious ones being access control, CCTV, burglar and fire systems," said Dave Warkentin, director of sales at Silent Witness, a video equipment monitoring manufacturer based in Vancouver, BC.

Warkentin echoed Wilson's observations: "We are also seeing a move toward having all the systems that are in a building being integrated," he said. "We're seeing

HVAC, lighting and all kinds of systems together. Companies want to be able to go to an end user or an owner and say, 'here is a system that can control everything—it's all integrated.'"

The challenge lies in complying with codes. "The technology has outpaced the ability of the code-making authorities to become comfortable with the code-making applications," Wilson said. "They are used to hard-wired systems and wiring configurations, and it's going to take time for us all to get comfortable with the reliability of a virtual network."

"The firm alarm platform has a UL requirement and a code requirement that other low voltage systems don't have," said David Ridder, contract services manager at Diversified Fire Products in Campbell, CA. "Fire alarms can't exist on open architecture; it's a closed system and closely regulated because it is a life safety system."

Maintaining a satisfactory level of security within these networks is also a prime concern. "As we migrate to an enterprise-wide network, I don't think any of us have enough history as to the amount of traffic that we are going to generate and develop on a network," Wilson said. "There are some issues surrounding security and proprietary information that people have to be comfortable with if they are allowing us to reside on that same network. We really have to be prepared as an industry, because there is a lot of risk involved in being part of an enterprise network."

Phil Libin, president of CoreStreet, a security products company based in Cambridge, MA, points to the blurring line between "physical" security and IT-based systems. "One of the most important factors is bridging the gap between physical and IT security—having sophisticated customers requiring the same system, the same level of thought, the same credentials go into both securing their data as well as their physical location."

In order to truly provide security, it's necessary to pay equal attention to both, Libin said. "You can spend a lot of money for the best IT security, but if your physical security is lacking, people can just walk in and physically steal your computers."

All of this requires a solid grasp of how to integrate these systems, and how they function on a day-to-day basis. Companies that are just beginning to explore this market must provide their personnel with adequate training to do the job.

"They need to have expertise in CCTV, burglar alarm, fire, etc., in order to develop these systems," Warkentin said. "A big challenge for the contractor is that someone has got to integrate and install these systems, and there are still fairly wide and varied requirements as far as the technical capabilities that are required to do this."

The proliferation of IP-based technology contributes to this issue. "What exacerbates the problem is CCTV and many other systems are moving toward IP connectivity," Warkentin said. "The future of CCTV is moving video over an IP network; the days of the analog CCTV business are numbered. That may take a few years, but that is absolutely where we are headed. Contractors must understand video, cameras, lighting and also how to build networks."

And if they do, they may reap the rewards. "The Web is bringing incredible changes and incredible opportunity," said Bill Bozeman, president and CEO of the PSA Security Network in Denver, CO. "The storage capabilities, off-site monitoring capabilities, and bandwidth compression has led to a whole new set of manufacturers, software developers and opportunities."

Many of these opportunities exist in the corporate market. "Through the expansion and growth of computers, corporate networks are able to view videos remotely from a number of different sites," said Frank Polidoro, national sales manager, Samsung

CCTV Systems in Secaucus, NJ. "The accessibility of broadband allows that to happen."

Nowadays, security systems aren't simply equipped to monitor specific sites; individual pieces of property may also be put under surveillance. The ability to track valuable items like laptop computers and high-end portable equipment is extremely attractive to organizations concerned with theft. "We are going to start seeing the use of technology where people can track inventory electronically, or track each and every piece of property over a certain dollar value," Wilson predicted. "I think the combination of that and integrating asset management into systems like access control systems will be the next application layer that will sit on top of today's current security technologies."

While at one time companies and public organizations shied away from being overtly secure, the climate these days is much different. "If you are looking at it from a perimeter point of view, the perimeter is no longer the front door of the lobby-it's 100 feet before you hit the door," said Tony Diodato, president of Cypress Computer Systems, an access control and security products company based in Lapeer, MI. "As part of their strategic planning, organizations are creating that layer around the building that you have to get through. That seems to be the trend with industrial companies and military bases."

"Our society is becoming comfortable with the concept of being under surveillance for our own protection, and I think that we tend to favor that as opposed to the privacy factor," Wilson said.

Carolyn Heinze works from her office in Vancouver, Canada.