# WITH POST-SEPT. 11 SYSTEMS IN PLACE, COMPANIES FINE-TUNE SECURITY EFFORT

## *SECURITY GUARD*

**By Chris Cziborr**
ORANGE COUNTY BUSINESS JOURNAL STAFF
07/11/2005

Corporate security may not be the hot button issue it was immediately following the 2001 terrorist attacks, but that doesn't mean companies are complacent.

John Wayne Airport: security spending has gone up dramatically for aviation, other sensitive industries

For one, large companies now are hiring seasoned chief security officers, said Scott Nelson, founder and president of Security & Risk Management Group LLC, a Westlake Village-based consulting company. He also teaches at the Costa Mesa campus of the University of Phoenix.

Nelson said companies have boosted their employee screening processes while some sensitive industries continue to boost spending on security.

Nelson was commissioned as a second lieutenant in the Marine Corps in 1965. He then served at the Army Special Forces Jungle School in Panama and later as a company commander and battalion operations officer in Vietnam.

For his service in the Vietnam War he received the Legion of Merit, Bronze Star, Purple Heart, Vietnamese Cross of Gallantry and Presidential Unit Citation. He also was promoted to the rank of captain.

Nelson became a special agent with the FBI in 1970. He worked at the FBI for more than 25 years.

After retiring from the FBI he became vice president of security for Warner Bros. Studios in Burbank and then Time Warner Inc. in New York.

At Time Warner, he led the company's Sept. 11 corporate response team in New York.

Nelson teaches courses in homeland security, organizational behavior, criminal justice, organized crime, ethics and policy matters at the University of Phoenix.

Following is an edited version of a Business Journal interview with Nelson.

How have things changed for companies since Sept. 11?

There really was a lot more interest in security after Sept. 11. For many companies there was a huge spike in security spending, but that has leveled off.

There still seems to be a concern, but companies by now have put systems in place, including cameras and alarms.

And they've hired more competent security directors. The new position is called chief security officer and that's helped for strategic planning.

One thing that big companies are doing is hiring very good chief security officers.

For a Fortune 500 company, I would say the salary range for such a position used to be $150,000 to $175,000. The range for a big company with international operations now is $250,000 to $350,000.

Companies have tended to cut back on card services and cameras and those physical security products where spending spiked right after Sept. 11.

I think what they're trying to do is use a combination of people and systems and strategies with a very good security director to protect the most critical assets as opposed to just protecting everything.

Right now we're saying, "Listen, you can't protect everything. You've got to figure out what's critical with your people and property and systems. Put your money there. Spend smart as opposed to spending randomly."

What are the main concerns for companies?

The first thing I tell all my clients is that they need to have a solid, practical security philosophy. For that you need to have a very energetic, cutting-edge security director.

The company needs to establish the philosophy of, "We will protect our people. We will protect our property. We will protect our information." And senior management needs to tune into this so they don't just give lip service to it.

Then you come up with practices, policies and procedures—those are where the rubber meets the road. That's where you put in your physical security systems like cameras and guards and alarms.

And then you put in procedural things for crisis management, business continuity and first responder issues.

A lot of this stuff is risk driven. Say you have a manufacturing operation that makes a low-cost product. You haven't had any thefts or incidents. The risk factor is such that you may not want to put a lot of security money into that.

On the other hand, if you're a financial institution and you run a cash center or have bank robbery problems at your branches, then the risk factor is high.

What I attempt to do is look at those items that maybe could be hugely disastrous but are highly unlikely—like weapons of mass destruction.

How probable is a nuclear attack? How much would it cost to protect against that?

So it sounds like security spending now is more on workers and procedures?

Yes, there is more focus on contingency planning, crisis management, business continuity and emergency preparedness.

Some people still are putting in cameras and alarm systems and that sort of thing. Some people are being very sophisticated.

Some key industries in the U.S. are highly protected. The spending—not for general businesses in Orange County—but for highly sensitive infrastructure industries like nuclear power and aviation and certain communication centers has gone up dramatically. But that's an anomaly—I don't think that's representative of companies across the board.

Industries like aviation and the nuclear power sector use armed guards and they have biometric sensors—things that most businesses really can't afford.

How do biometrics work?

A biometric indicator can be a fingerprint, a voice recognition device or an eye scan.
If it's a thumbprint, for example, you put your thumb on a reader and the database records your print and checks against all the prints of those who have authorized access. Or it reads the iris/retina of the eye. It reads the composition and the texture of the eye just as it would a fingerprint.

We also have companies that went to electronic card readers over the years, where you pass or swipe a card to get access to a locked door.

In some cases companies might use all of the above.

You might have a highly secured area or a cash center that might have a regular brass key entry and it would have a card access system and then biometric. It would have layers. We probably never will completely get away from the brass key concept. It sounds nice to have everything electronic but it's very expensive.

What about legal concerns with background checks?

Liability often drives the ship.

For example, if you hire an employee that has a criminal record of fraud and assault, comes on the job and assaults an employee, then there will be major liability concerns for a company.

It behooves companies to screen their employees properly and that includes criminal/civil and sometimes driver's license and background reference checks.

It's a moneymaker for companies, because it's much easier to reject a person in advance of employment.

Once a person is on board it's much more difficult to terminate that employee unless it's for direct cause.

And the other issue in the workplace is the issue of safety and security and having reasonable systems in place to ensure that people are safe and secure.

There also are liability issues in safety and security—having reasonable methods and procedures in place to ensure that visitors and employees are safe.

University of California, Irvine, has started a state-mandated course that teaches guards how to identify weapons of mass destruction and terrorists. Is that helpful?

It's all helpful.

UCI's four-hour training for terrorist recognition is fine in addition to other training. The guard's job is to observe and report. They are not FBI agents. They are not experts in the field.

But if you get a good guard with good eyes and ears, excellent training and a good background check—the more education they have the better.

California already requires some 40 hours of certification for security guards. California is more advanced than many states. Some don't have any requirements.

In some states a 7-Eleven clerk or a kid with a long felony record can become a guard at a sensitive location. But in California the (check) system is pretty advanced.

The Department of Homeland Security also has a program for truckers that trains them to be the eyes and ears. That's very good, because truckers are all over the place.

It raises the question of "do we tell on our neighbors," but frankly that has all changed with Sept. 11.

The community must get involved with prevention.

Do you work with international companies?

I work with a number of very large financial institutions—some have businesses based in OC or have operations here. They have international operations that include manufacturing and call centers in places like India.

Places like India provide an interesting environment. Studies show that the call centers in India are subject to identity theft. You can hire vendors and contract out and teach people how to speak English and process the slang and the needs of the company. But whether you can overlay information protection systems on foreign vendors—whether that's effective—is a big issue.

Frankly, we've seen that there have been a lot of problems in India in that very area.

How so?

We've found that the privacy of records with some vendors and contractors in India hasn't been protected as well as it should.

We're also having problems in the U.S.—we're not doing a very good job protecting information here either.

I'm a former Time Warner vice president and it's been publicly acknowledged that Iron Mountain—a company that stores their data—lost data on several hundred thousand names, probably including mine.

So we in America aren't doing a very good job of keeping our data secure. But we're working very hard. Federal and state authorities are putting out regulations right and left. It's been a frenzy of regulatory activity, which is fine and it's needed. Private information should be protected.

But overseas operations are especially tough—they're tough to manage and difficult to superimpose regulations on.

Have you dealt with a company that had operations in a politically or militarily unstable region?

Yes, in Mexico we've had huge issues with danger, with individuals along the border, kidnappings and murders.

And also we've had big issues with use of transport systems to carry drugs back and forth between Mexico and the U.S.

The border issues today between the U.S. and Mexico are huge. They involve public safety, police corruption and transportation of drugs north. It's tough and of course a lot of businesses are setting up manufacturing plants in Tijuana and Laredo and other areas because of the cost of doing business.

I have done business in Europe too.

What I end up doing is utilizing a vast network of FBI, CIA and state and local folks around the world. I subcontract out a lot of my investigations work. If I have an investigative thing for fraud or embezzlement, I go to the FBI. If I have a drug issue, I will get in touch with the Drug Enforcement Agency.

How does someone become a chief security officer?

Two ways. There's the professional law enforcement track, which is FBI or state local law enforcement. And then there's the security practitioner track. That's maybe somebody who's worked his or her way up through a security company like Kroll or Guardsmart.